Some Algebraic and Number Theoretic Aspects of Classical and Post Quantum Cryptography

Author: Ankan Pal
Thesis Advisor: Prof Norberto Gavioli

Thesis Abstract.

In this thesis, the focus is on studying some of the mathematical aspects in the perspective of contemporary issues in information security. Post-quantum era is round the corner and it is not anymore a far-fetched reality. In post-quantum cryptography, we discuss the design of a new digital signature algorithm using isogenies of supersingular elliptic curves over a finite field. In classical cryptography, we discuss a novel geometric interpretation of the elliptic curve discrete logarithm problem, and the application of recursive towers for producing high order elements in finite fields. Another concept which is explored in the thesis is estimation of class numbers, which is necessary for designing secure cryptosystems over number fields.

About.

Ankan Pal. The author of the thesis, Ankan Pal is presently a doctoral student at University of L'Aquila, Italy. His primary research interests are Cryptography and Number Theory. Prior to his journey into Mathematics, he graduated as a Mining Engineer and worked for four years in various academic and non-academic positions. He is enthusiastic, and considers himself as an amateur philosopher and a dexterous orator. In this thesis, he discusses cardinally about some of the mathematical problems that arise in the field of Cryptography.

Prof Norberto Gavioli. The advisor of this thesis, Prof Norberto Gavioli is working as an Associate Professor at the University of L'Aquila, Italy. He is an accomplished researcher in the field of Group Theory. His primary research interests lies in p-groups. He also has a keen interest in the field of Cryptography. He has published many research papers in various prestigious journals.

Legalities.

The thesis includes results from unpublished works of Ankan Pal and his collaborators. It can only be used (with appropriate references), after obtaining the prior approval of the respective authors of the unpublished work.

Disclaimer 0.1. The thesis is an amalgamation of many concepts from various sources. A detailed bibliography is provided at the end of the thesis for all the references. In this disclaimer, we notify that many parts of the chapters are *collated from the mentioned books/research papers of various authors OR pre-prints/unpublished works of Ankan Pal, with no/little changes*, with some of Ankan Pal's commentaries, remarks, and observations. Standard symbols and definitions are kept intact for greater reliability and readability. This is the full disclaimer which is mentioned for the reference(s), as some of the concepts/terms/definitions are used in the thesis from the respective sources. Please note that other references are mentioned wherever necessary.

Color Code.

Online References/Web-Links.

Cross References within the document.

References in the Bibliography.

UNIVERSITÀ DEGLI STUDI DELL'AQUILA

DIPARTIMENTO DI INGEGNERIA E SCIENZE DELL'INFORMAZIONE E MATEMATICA

Dottorato di Ricerca in Matematica e Modelli

XXXII ciclo

Titolo della tesi

Some Algebraic and Number Theoretic Aspects of Classical and Post Quantum Cryptography

SSD MAT/02

Dottorando

Ankan Pal

Coordinatore del corso

Prof. Davide Gabrielli

Tutor

Prof. Norberto Gavioli

A.A. 2018/2019

Contents

Main Results

The major objective of this research work is to explore some of the algebraic and number-theoretic aspects of mathematical cryptography. The work can be categorized in many ways. But, the major aim is two-fold, either, to come-up with quantum-resistant cryptographic methods or to strengthen the existing classical cryptography. Chapter 4 on Isogeny-based Cryptography is towards the *quantum-resistant* objective. Chapter 2 and 3 are about strengthening the existing cryptographic methods for a smooth transitioning into a post-quantum era. Only chapter 1 is about *cryptanalysis*, which deals with a probable *attack* on elliptic curve cryptography. These research themes are explored, and in the process various mathematical ideas are developed. Now, we provide a preview of the main results of the the thesis which would help a reader to navigate through the thesis.

1. *Geometric Interpretation of Elliptic Curve Discrete Logarithm Problem*

This is a joint work of the PhD candidate Ankan Pal with Daniele DiTullio, which is completed and available online on arXiv.

The main objective of this work was to understand the geometric interpretation of Elliptic Curve Discrete Logarithm Problem (EC-DLP) (def 1.2.3). EC-DLP is at the core of the elliptic curve Diffie-Hellman key exchange (subsection 1.2.3) in *Elliptic Curve Cryptography* (ECC).

Let, E be an Elliptic Curve (def 1.2.1) over a finite field $\mathbb{F}_p$ of characteristic p, for some prime $p \geq 5$. Let, points P and $Q \in E$ and $n \in \mathbb{Z}/N\mathbb{Z}$, where N is the order of the point P. We can define the EC-DLP in this setting as, $Q = nP$, where $n < \#E$. It is a computationally hard problem to compute n, even if P and Q are known. If we view this operation geometrically, then it is the intersection of a line with the elliptic curve (fig. 1). Hence, EC-DLP can be viewed as this operation performed n times. Hence, if we want to compute the value of n, we need to understand this multiple intersection in detail. We set out to understand and explore this interpretation of EC-DLP, in this project.

In his seminal work [Sema04], Igor Semaev came up with the idea of summation polynomials (def 1.3.1), which has been proved to be effective in designing attacks on EC-DLP when coupled with Weil Restriction (def 1.3.2). This is an interesting idea, but the major impediment in the computation of summation polynomials is finding an effective way to evaluate resultants over the algebraic closure of $\mathbb{F}_p$.

We were successful in averting the explicit calculation of resultant by our method. But, in the end, when we designed the attack on EC-DLP, we arrived at over-determined system of equations, which arose due to the intersection of quadrics. We tried to solve these over-determined system

of equations with the help of Faugere $F4$ algorithm [Faug99] on MAGMA computer algebra system. *They were computationally hard to solve, and we realized that when compared with the existing strategies; the intersection method is only useful for designing attacks on EC-DLP for the elliptic curves on fields having small characteristic* ($4 < p < 500,000$). We developed an *Intersection Method* algorithm (Appendix A) to verify our attack strategy.

The main result deals with the evaluation of valuation *(multiplicities)* (def 1.4.1) at the intersection of an affine curve C and the elliptic curve E. The valuation v, at the intersection is expressed in terms of the *intersection number* [Ful08]. The intersection number of the two curves C and E at point P_0 is denoted by $(C \cdot E)_{P_0}$. The proof is done in two steps, by taking different scenarios of intersection of these curves. The statement of the main result on intersection of curves (theorem 1.4.2) is stated here.

Theorem (Intersection of Curves). Let, $E : y^2 - (x^3 + Ax + B)$ be an Elliptic Curve over a finite field $\mathbb{F}_p$ of prime characteristic $p \geq 5$, and $C : f(x, y) = 0$ be an affine curve. Let, $r(x) := \mathrm{Res}_y(f(x, y), y^2 - (x^3 + Ax + B))$ be the resultant, and $P_0 = (x_0, y_0) \in E$. Then the valuation is,

$$v_{(x-x_0)}(r(x)) = (C \cdot E)_{P_0} + (C \cdot E)_{-P_0}.$$

In chapter 1, we start with a basic introduction to elliptic curves and then move on to summation polynomial based attacks on EC-DLP. This provides the necessary motivation and background for our research work. The new results are provided in section 1.4. In this section, the main result is Theorem 1.4.2 on Intersection of Curves. In subsection 1.4.2, we have described the design of an attack strategy on EC-DLP. We conclude with some remarks on this attack methodology in section 1.5.

2. *High Order Elements in Finite Fields Arising from Odd Recursive Towers*

This is a joint work of the PhD candidate Ankan Pal with Valerio Dose, Pietro Mercuri, and Claudio Stirpe. This work is completed and available online on arXiv.

Finding effective ways to search primitive elements in finite fields has been an interesting topic in Computational Number Theory. These effective search algorithms can then be utilized for finding high order (*near primitive*) elements, which can be useful in posing difficult or more secure discrete logarithm problem (def 1.2.2). A literature survey on this aspect has been provided in section 2.2.

One of the elementary ways that can be useful in constructing elements in a finite field is through recursion. Some expository examples of this aspect can be found in [MuPa13]. In this research work, the major objective was to find meaningful polynomial relationships for recursion, and then use these relationship in a tower of fields (called as *recursive towers*), to find high order

elements.

Let p be an odd prime. Let $k \in \mathbb{Z}$ be a non-negative integer, by $\mathrm{GF}(p, 2^k)$, we will denote a field having p^{2^k} elements. By tower of fields, or simply a tower, we mean a sequence of field extensions

$$K_1 \subset K_2 \subset \ldots \subset K_n \subset \ldots,$$

All the towers we consider are *finite, normal and separable*, i.e., each extension K_n/K_{n-1} is finite, normal and separable, for every $n > 1$. For each positive integer n, let the extension $K_n = \mathrm{GF}(p, 1)[x_n]$, where the element $x_n \in \mathrm{GF}(p, 2^n)$ is given by a recursive formula $f(x_{n-1}, x_n) = 0$, for a polynomial $f(x, y) \in \mathrm{GF}(p, 1)[x, y]$. In this case, we say that the tower $K_1 \subset K_2 \subset \ldots \subset K_n \subset \ldots$ is defined by $f(x_{n-1}, x_n)$ and we address this kind of towers as recursive towers. We focus on towers defined by $f(x_{n-1}, x_n) = x_n^2 + x_n - v(x_{n-1})$, for $n \geq 2$, with $x_1 \in \mathrm{GF}(p, 2)$, and where $v(x)$ is a polynomial in $\mathrm{GF}(p, 1)[x]$. We denote by δ_n the discriminant $\delta_n = 1 + 4v(x_n)$, for $n \geq 1$. Given the tower defined by $f(x_{n-1}, x_n)$, we denote by $g(x, y) \in \mathrm{GF}(p, 1)[x, y]$ a polynomial giving the relation between two consecutive discriminants δ_{n-1} and δ_n, namely $g(\delta_{n-1}, \delta_n) = 0$.

Remark. Whether the characteristic of the finite field is even or odd, we say that the tower is odd or even. In the thesis we will only consider the towers in odd characteristic. By good towers K_n, we will refer to those towers for which high order elements can be constructed through the recursive form of $f(x_n, x_{n-1})$.

In order to find good towers we restrict our search to polynomials $f(x, y) = y^2 + y - v(x)$, with $v(x) \in \mathrm{GF}(p, 1)[x]$ being a non-zero polynomial, which satisfy Condition **(1)** below, and at least one condition out of **(2)** or **(2′)**.

(1) $\frac{f(x_{n-1},0)}{x_{n-1}}$ is a square in $\mathrm{GF}(p, 2^{n-1})$ for $n \geq 2$;

(2) $\frac{g(\delta_{n-1},0)}{x_{n-1}}$ is a square in $\mathrm{GF}(p, 2^{n-1})$ for $n \geq 2$;

(2′) $\frac{g(\delta_{n-1},0)}{\delta_{n-1}}$ is a square in $\mathrm{GF}(p, 2^{n-1})$ for $n \geq 2$.

The following theorem ensures that all the polynomials $f(x_{n-1}, x_n)$ listed in section 2.3.2 define towers of fields. In particular it shows that $[K_n : K_{n-1}] = 2$, for all $n > 1$.

Theorem. Let $v(x) \in \mathrm{GF}(p, 1)[x]$ be a polynomial and assume that $f(x_{n-1}, x_n) = x_n^2 + x_n - v(x_{n-1})$ satisfies Conditions **(1)** *and* **(2)**, or Conditions **(1)** *and* **(2′)**. If x_{n-1} and δ_{n-1} are not squares in the multiplicative group $\mathrm{GF}(p, 2^{n-1})^*$ for a suitable $n \geq 2$, then x_j and δ_j are not squares in the multiplicative group $\mathrm{GF}(p, 2^j)^*$, for $j \geq n$.

As a corollary to the aforementioned theorem, we prove the following about the lower bound of the order of elements.

Corollary. Let $v(x)$ be a polynomial in $\mathrm{GF}(p,1)[x]$ and assume that $f(x_{n-1}, x_n) = x_n^2 + x_n - v(x_{n-1})$ satisfies Conditions **(1)** and **(2)**, or Conditions **(1)** and **(2')**, and that x_1 and δ_1 are not squares in $\mathrm{GF}(p,2)$. Then $x_n^2 \notin \mathrm{GF}(p, 2^{n-1})$ and the order of x_n is greater than

$$2^{\frac{1}{2}(n^2+3n)+\mathrm{ord}_2(p-1)-2},$$

for all $n > 1$. The same lower bound also holds for the order of δ_n if $\delta_n^2 \notin \mathrm{GF}(p, 2^{n-1})$ for all $n > 1$.

The proofs of these results are provided in section 2.3 of chapter 2, which uses basic techniques from Algebraic Number Theory. The proving mechanism is inspired from [*BCGH*+09]. We present the Recursive Tower Algorithm (implemented on MAGMA) in Appendix B. The algorithm could produce elements of the order 2^{1771}, in less than 650 seconds, which is comparable to the state of the art results, and much higher than the lower bound mentioned in the corollary. The Numerical Results are provided in Appendix C.

Note. In this thesis, we have used an odd prime p for the construction of towers and proving their subsequent properties. We have given the numerical results for the same. But, this can be generalized for any **prime power**. In this thesis, we have dealt with odd recursive towers. The *even* case is even more interesting as the properties can be derived in similar ways, but there is a need to prove some basic properties using Cardano's formula and elementary Galois Theory. In the research paper titled *High Order Elements in Finite Fields Arising from Recursive Towers* by Valerio Dose, Pietro Mercuri, Ankan Pal (the PhD candidate), Claudio Stirpe; we have also dealt with the even recursive towers.

3. *Class Number Estimation*

Estimation of Class Number (def 3.3.2) is vital for designing of secure cryptograhic primitive on Number Fields. **Dirichlet** found a remarkable class number formula while studying quadratic forms. The formula was expressed in terms of Kronecker symbol. If we consider only imaginary quadratic fields $\mathbb{Q}[\sqrt{-p}]$ of prime discriminant $p > 3$, such that $p \equiv 3 \ (mod\ 4)$, then the formula can be further simplified, and can be expressed in terms of Legendre symbol. In this research work, in theorem 3.3.2, we take a step further and express it in terms of sums, which *might* result in computational efficiency. We derive the following formula by using the transformation formulas given by KS Williams in [Will70].

Theorem (Class Number Estimation). Let $p > 3$ be a prime, and h_p be the class number of a quadratic imaginary number field $\mathbb{Q}[\sqrt{-p}]$. We set,

$$h_p^* := \begin{cases} 0 & p \equiv 1 \mod 4 \\ h_p & p \equiv 3 \mod 4. \end{cases}$$

Then,

$$h_p^* = \frac{p-1}{2} - \frac{2}{p}\left(\frac{(\lfloor \sqrt{p} \rfloor)(\lfloor \sqrt{p} \rfloor + 1)(2\lfloor \sqrt{p} \rfloor + 1)}{6} + \sum_{x=\lceil \sqrt{p} \rceil}^{\frac{p-1}{2}} (x^2)_{mod\ p} \right).$$

Note. The sum $S = \sum_{x=\lceil \sqrt{p} \rceil}^{\frac{p-1}{2}} (x^2)_{mod\ p}$ is a peculiar sum and it can be abbreviated as **SMPS** (**Square** each element then **mod p** then **Sum**).

4. *Supersingular Isogeny-Based Designated Verifier Blind Signature*

This is a joint work of the PhD candidate Ankan Pal with Agnese Gini, and Rajeev Anand Sahu. This work is completed and available online on IACR.

Isogeny based Elliptic Curve Cryptosystems are one of the candidates for post-quantum cryptography. An undeniable blind signature scheme constructed by utilizing isogenies of supersingular ellipic curves was proposed by Srinath et al [SrCh16] to provide signer's control in a quantum-resistant blind signature scheme. In this, neither the requester nor the signer can determine a selected verifier apriory. Furthermore, certain weaknesses of undeniable signatures have already been observed and have been overcome by the proposal of designated verifier signature in the classical setting. Following these motivations, we present a quantum-resistant designated verifier blind signature scheme based on supersingular isogenies, in section 4.3 and 4.4. Our construction does not require interactive communication between the signer and the verifier. However, it involves the signer in the verification. This idea of a quantum-resistant blind signature might be useful in specific applications, for example in electronic tendering and online auctioning.

Note. In 2020, this research work got *five* citations. [KMPPS20] is one of the research papers, which cited our work. The proposed signature scheme has some weaknesses against the attacks designed by Kutas et al in [KMPPS20]. In this thesis, we have elucidated the novel two-cube method, to illustrate that how isogenies of the supersingular elliptic curves can be utilized for designing a blind digital signature with a designated verifier. In the research paper titled *Supersingular Isogeny-Based Designated Verifier Blind Signature* by Rajeev Anand Sahu, Agnese Gini, and Ankan Pal (the PhD candidate); we have discussed the security proofs. But, the mentioned Digital Signature is not *yet* strong enough to ward off the threats posed by the attacks designed by Kutas et al in [KMPPS20].

Chapter 1

Geometric Interpretation of Elliptic Curve Discrete Logarithm Problem

Note 1.0.1. This chapter entails the results from the research paper titled *A New Method for Geometric Interpretation of EC-DLP* by Daniele Di Tullio and Ankan Pal (the PhD candidate). To read the full reference disclaimer, please refer to [0.1].

1.1 Chapter Description

In this research work, we studied a geometric interpretation of the Elliptic Curve Discrete Logarithm Problem (EC-DLP). The key idea is to reduce EC-DLP into a system of equations. These equations arise from the intersection of quadric hypersurfaces in an affine space of lower dimension. In cryptography, this interpretation can be used to design attacks on EC-DLP. One of the widely studied attack algorithm uses the concept of Summation Polynomials and Weil Descent. Summation Polynomials needs the calculation of resultants of polynomials which is a computationally heavy task. To avoid this, we proposed this new geometric interpretation. Although, our method avoids the computation of summation polynomials explicitly, but it produces over-determined system of equations, which are hard to solve. Hence, conclusively we can only claim that our method is only useful for elliptic curves defined over finite fields of small characteristic (primes greater than 4 and less than $500,000$). The statement of the main result (theorem 1.4.2) is as follows.

Theorem (Intersection of Curves). Let, $E : y^2 - (x^3 + Ax + B)$ be an Elliptic Curve over a finite field $\mathbb{F}_p$ of prime characteristic $p \geq 5$, and $C : f(x, y) = 0$ be an affine curve. Let, $r(x) := \text{Res}_y(f(x, y), y^2 - (x^3 + Ax + B))$ be the resultant, $P_0 = (x_0, y_0) \in E$, and $(C \cdot E)_{P_0}$ be the *intersection number*. Then the *valuation* (def. 1.4.1) can be evaluated as,

$$v_{(x-x_0)}(r(x)) = (C \cdot E)_{P_0} + (C \cdot E)_{-P_0}.$$

This chapter starts with a gentle introduction to the group structure of Elliptic Curves in subsection 1.2.1. The group structure is required for defining elliptic curve discrete logarithm problem in subsection 1.2.2. Thereafter, an attack on EC-DLP is described in subsection 1.3.1. This method relies heavily on computing the summation polynomials (def. 1.3.1). This reliance is avoided and a new method for attacking EC-DLP is elucidated in this chapter. The novelty of this method is that it relies/appeals to the geometric characterization of elliptic curves. The main result that is proven in this chapter is theorem 1.4.2. The proof is done in *two* steps, by taking different scenarios of intersection of curves. This result is about intersection of curves. This result is utilized in subsection 1.4.2 to design an attack on EC-DLP. An algorithm for the Intersection Curve Method implemented in MAGMA [BoCa93] is provided in Appendix A. The last section of the chapter draws some conclusions on this research work.

Remark 1.1.1. The major drawback of the intersection method is that it produces over-determined system of equations which have high time complexity. We have used Grobner basis (refer definition 1.3.3) and $F4$ (Faugre) algorithm [Faug99] to solve these system of equations. The characteristic p of the field $\mathbb{F}_p$ over which the Elliptic Curve E is defined, plays a crucial role on the efficiency of the algorithm. The method produces sub-optimal results for large primes, even with substantial computational power. For primes less than $500,000$, the intersection method produces optimum result.

1.2 Elliptic Curves and Discrete Logarithm Problem

Definition 1.2.1 (Elliptic Curve [Sil09])**.** An elliptic curve $E(\mathbb{K})$ over a field $\mathbb{K}$, is a non-singular projective curve of genus **one** with a specified base point, known as the point at infinity O, such that $O \in E(\mathbb{K})$.

For practical purposes, elliptic curves can be thought of as plane non-singular cubics with fixed Weierstrass co-ordinates. The generalized Weierstrass equation can be deduced using Riemann-Roch Theorem.

$$y'^2 + a_1x'y' + a_3y' = x'^3 + a_2x'^2 + a_4x' + a_5 \tag{1.2.1}$$

Generalized Weierstrass Equation

Where, $a_1, a_2, a_3, a_4, a_5 \in \mathbb{K}$. If characteristic of the field is not equal to 2 *or* 3. Then, after some algebraic manipulation, we get:

$$y^2 = x^3 + Ax + B.$$

Where, $A = a_4{}' - \frac{a_2'^2}{3}, B = a_5{}' - \frac{a_2{}'a_4{}'}{3}, x = x' + \frac{a_2'}{3}, y = y' + \frac{a_1x'}{2} + \frac{a_3}{2}$.

Remark 1.2.1. The definition is vague until we define a group structure on it, which in-turn is the reason for the rich algebraic properties of Elliptic Curves.

1.2.1 Group Structure of Elliptic Curves

For the group structure on elliptic curves, we need a way to do operations on the points of the curve. We start by describing the idea of Tangent-Chord operation and then use basic techniques to understand the group structure. For notational convenience, we will denote a field by $\mathbb{K}$, and $E(\mathbb{K})$ be an elliptic curve over it, and P be a point on $E(\mathbb{K})$. Many ideas for this subsection were taken from the book titled "*Elliptic Curves: Number Theory and Cryptography by LC Washington*" [Wash03].

Point Addition (Tangent-Chord Operation) [El18].

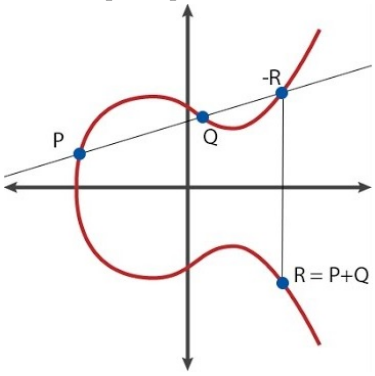


Figure 1: Point Addition [El18]

We will describe the operation $+_{tangent-chord}$, and how $P(x_1, y_1) +_{tangent-chord} Q(x_2, y_2) = R(x_4, y_4)$. From the figure, we have $P, Q, R, -R$ are points on $E : y^2 = x^3 + Ax + B$. We join PQ and extend the line ℓ to intersect E on another point $-R(x_3, y_3)$. Hence, the slope of the line is, $m = \frac{y_2 - y_1}{x_2 - x_1}$. So, the equation of the line ℓ is, $y = m(x - x_1) + y_1$. Hence, we have, $(m(x - x_1) + y_1)^2 = x^3 + Ax + B$. Rearranging, we get: $x^3 + (-m^2)x^2 + (A - 2my_1 + 2m^2x_1)x + (B - {y_1}^2 + 2my_1x_1 - m^2{x_1}^2) = 0$. Since, sum of the roots of this equation is m^2. So, $x_1 + x_2 + x_3 = m^2$ or $x_3 = m^2 - (x_1 + x_2)$. Putting this in the equation of the line ℓ we get: $y_3 = m(x_3 - x_1) + y_1$. Now, we reflect $-R(x_3, y_3)$ along the abscissa, and letting $x_4 = x_3$, and $y_4 = -y_3$, we get the point $R(x_4, y_4)$.

Note 1.2.1. This point addition is known as the *tangent-chord* operation. From now on, we will denote $+_{tangent-chord}$, simply with a $+$, to signify the addition of the points on an Elliptic Curve.

Do the points on elliptic curve form an Abelian group? Let, $P_1, P_2, P, -P \in E(\mathbb{K})$. The line joining P_1 to P_2 is same as the line joining P_2 to P_1. Hence, the commutativity of the tangent chord operation can be derived. The point at infinity O, acts as the *identity* element for the group $E(\mathbb{K})$, since, $P + O = P$. Let, P be an arbitrary point (x, y) on E and $-P = (x, -y)$. If we join these two points, then it gives us a straight line which intersects the curve E at the point at infinity O. Hence, there exists inverses, since, $P + (-P) = O$. An interesting point to note is that we are considering the point at infinity $O \in E(\mathbb{K})$, hence a line will always intersect E at three points. So, the described point addition always generates a point in $E(\mathbb{K})$. Hence, for every point on an elliptic curve, the point addition is closed and commutative. Apart from associativity, the other properties are derived in a straight-forward manner. We provide a small illustration on the associativity of the operation.

Associativity of the Tangent-Chord Operation: The well known *Chasle's and Bezout's Theorem* [Huse87] can be used to prove associativity of the tangent-chord method. The following figure provides a visualization of the idea.

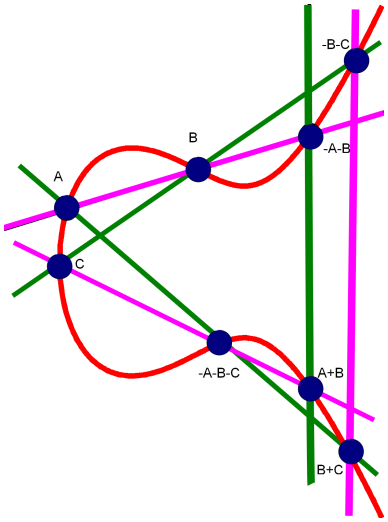


Figure 2: Associativity[1]

Sketch of Proof of Associativity [Huse87]: Although the figure entails the details of associativity, it is not a straightforward consequence. We need to prove that $\forall\ A, B, C \in E$, we get $(A + B) + C = A + (B + C)$. Hence, we need to prove that $(A + B) + C - (A + (B + C)) = \mathcal{O}$. To prove this we need **Chasle's Theorem**. We can assume that the 8 points (shown in the figure) are the intersection points. If we assume that and apply Chasle's theorem, we can clearly see that the 9th point $-((A + B) + C)$ would coincide with $(A + B) + C$. This would prove that the two points are the same. This would imply associativity and prove that the points on an elliptic curve form a Group. This Group Law is not only true for elliptic curves defined over $\mathbb{C}$ but also elliptic curves defined over $\mathbb{Q}$, $\mathbb{F}$, and their finite/algebraic extensions.

By the above arguments, it is evident that Elliptic curves over finite fields $\mathbb{F}_p$ form a group. One of the initial estimation of the order of this group or the number of points on the elliptic curve $\#E(\mathbb{F}_p)$, was given by **Hasse**, which we mention here.

Theorem 1.2.1 (**Hasse's Theorem**[Wash03])**.**

$$p + 1 - 2\sqrt{p} \leq \#E(\mathbb{F}_p) \leq p + 1 + 2\sqrt{p}.$$

Group structure of elliptic surves is one of the fundamental algebraic aspects of elliptic curves, which enables us to implement many ideas. Hence, it is included in the thesis as an illustrative/descriptive subsection.

1.2.2 Elliptic Curve Discrete Logarithm Problem

Elliptic curves over a finite field $E(\mathbb{F}_p)$ essentially are rich mathematical structures which result in their ubiquitous use in Number Theory and Cryptography. Elliptic Curve Discrete Logarithm Problem (EC-DLP) has myriad applications and it is used to design many of the classical cryptosystems involving elliptic curves.

Definition 1.2.2 (*Discrete Logarithm Problem (DLP)*)**.** Let, G be a group and $a, b \in G$. Suppose we know that there exists an integer k such that, $a^k = b$, then Discrete Logarithm Problem is about finding k, for given a and b.

Uses of DLP [PaPe09]:

- Encryption-Decryption
- Key Exchange
- Digital Signatures

[1]Retrieved from https://terrytao.wordpress.com on December 03, 2019.

DLP needs a Cyclic Group or a Cyclic Subgroup. But then why to use Elliptic Curves?

Problem Posed	Cryptosystem	SL(128-Bit)	SL(256-Bit)
Factorization ($\mathbb{Z}$)	RSA	3072	15360
DLP ($\mathbb{Z}_p^*$)	DH, ElGamal, DSA	3072	15360
EC-DLP	EC-DH	256	512
Symmetric Key	AES, DES	128	256

The table is collated from [PaPe09]. From this table, we can deduce that EC-DLP is computationally more efficient, and hence used extensively in our Smartphones and Tablets. Another advantage of EC-DLP is that, it is difficult to design powerful attacks for EC-DLP.

Definition 1.2.3 (*Elliptic Curve Discrete Logarithm Problem (EC-DLP) [PaPe09]*)**.**

$$dP = T.$$

$$Find \;\; d.$$

Where, $P, T \in E(\mathbb{F}_p)$, d is a natural number which is the private key ($1 \leq d \leq \#E(\mathbb{F}_p)$), and T is the public key.

Remark 1.2.2 ([PaPe09]). Geometrically, the question posed is that 'in how many 'Hops" can one go from P (initial point) to T (final point).

1.2.3 Elliptic Curve Diffie Hellman Key Exchange

The objective of Elliptic Curve Diffie Hellman Key Exchange (EC-DH-KE), is that Alice and Bob want to exchange a key over an insecure channel. In the set-up phase, we have an elliptic curve $E : y^2 = x^3 + Cx + D \; (mod\ p)$ and a point $P = (x_P, y_P)$. In the protocol we use randomly generated number a and b to be the private key of Alice and Bob, respectively. $A = aP$ be the public key of Alice and $B = bP$ be the public key of Bob. Alice and Bob do the following communication:

$$A \rightleftarrows B$$

Now, the question is that *why* does EC-DH-KE works?. Alice computes $a(B) = abP$ and Bob computes $b(A) = baP$. Since, $abP = baP$. Hence, Alice and Bob both have the same point (x_{AB}, y_{AB}) with them. They now may decide to choose y_{AB} as their key. In this way, they do the key exchange in a secure way, assuming that EC-DLP is safe.

1.3 Summation Polynomial based Method

This section provides a preliminary sketch of *Summation Polynomial* based attacks on EC-DLP. Initially, index calculus methods [Wash03] were used to attack EC-DLP. The major impediment to such attacks was to find a computationally optimized factor base $\mathcal{F}$ (a set of elements having small logarithms). There were considerable improvements in this direction using baby-step-giant-step method. In the case, in which the cardinality of the set of rational points of the elliptic curve, is a smooth number, the Pohlig-Hellman attack [Wash03] is quite efficient. Pollard's ρ and λ methods were another approach for designing the attacks [Poll78]. In the case of supersingular elliptic curves (def 4.2.8), attacks were designed using Weil Paring, known as MOV Attacks [MOV93]. In other cases, EC-DLP is still hard to attack.

Presently, one of the widely studied attack algorithm having a sub-exponential time complexity for particular cases is through the implementation of Summation Polynomials and Weil Descent [GaSm99] [Sema04] [Diem13] [Gaud09]. In his seminal research paper of 2004, Semaev [Sema04] constructed summation polynomials to solve EC-DLP. Grobner basis was used for solving the system of equations that arose from such problems. A working attack algorithm of sub-exponential time complexity for small dimensions was developed by Gaudry [Gaud09], using the concepts of Summation Polynomials and Weil Restrictions. We illustrate the concept of *Summation Polynomials* in the next subsection.

1.3.1 Summation Polynomials

Definition 1.3.1 (*Summation Polynomials* [Sema04])**.** Let, $n \geq 2$, $\mathbb{F}$ be a Field such that $Char(\mathbb{F}) \neq 2, 3$, and E be an Elliptic Curve over $\mathbb{F}$, whose equation is given by $y^2 = x^3 + Ax + B$. Let, $f_n = f_n(X_1, X_2...X_n)$ be a Polynomial in n Variables, and $x_1, x_2, ..., x_n$ be any elements from $\overline{\mathbb{F}}$ (algebraic closure of the field $\mathbb{F}$). Then, f_n is called a Summation Polynomial if it satisfies the following condition.

$f_n(x_1, x_2, ...x_n) = 0$ if and only if there exists $y_1, y_2, ..., y_n \in \overline{\mathbb{F}}$, such that (x_i, y_i) are points on the elliptic curve E, and $(x_1, y_1) + (x_2, y_2) + ... + (x_n, y_n) = O$ in the group $E(\overline{\mathbb{F}})$.

Remark 1.3.1. The coefficients of these polynomials belong to the field $\mathbb{F}$. Definition 1.3.1 is a general definition and the underlying field $\mathbb{F}$ does not have to be necessarily a finite field. Although, in the subsection we are only concerned with applying this concept to design attacks on EC-DLP, which is modeled using the points of an elliptic curve over a finite field.

Theorem 1.3.1 (*Summation Polynomial Theorem* [Sema04])**.** *The summation polynomial f_n is,*

$$f_n(X_1, X_2, ..., X_n) = Res_X(f_{n-k}(X_1, ..., X_{n-k-1}, X), f_{k+2}(X_{n-k}, ..., X_n, X)),$$

for any $n \geq 4$ *and* $n-3 \geq k \geq 1$.

For $n = 2$, *we have* $f_2(X_1, X_2) = X_1 - X_2$, *and for* $n = 3$, *we have* $f_3(X_1, X_2, X_3) = (X_1 - X_2)^2 X_3^2 - 2((X_1 + X_2)(X_1X_2 + A) + 2B)X_3 + ((X_1X_2 - A)^2 - 4B(X_1 + X_2))$.

In the year 2000, approaches which use tools from Algebraic Geometry to design attacks on EC-DLP, were presented by Galbraith and Smart [GaSm99]. We provide a general definition of *Weil Restrictions* to provide a holistic flavor to the topics discussed in this section. We will **not** be using Weil Restrictions in the proof of our main result.

Definition 1.3.2 (*Weil Restrictions* [Hart13])**.** Let, $S' \rightarrow S$ be a map of schemes and let X' be an $S'-$scheme. Consider the functor on $S-$schemes $T \rightarrowtail X'(T \times_S S')$. If this functor is representable by an $S-$scheme X, we call X the restriction of scalars (or Weil restriction of scalars) of X from $S' \rightarrow S$, and denote it by $W_{Res_{S'/S}}(X')$.

Remark 1.3.2. When this functor is representable, we will say that $W_{Res_{S'/S}}(X)$ "exists". Any two schemes representing the functor are uniquely isomorphic in a manner which preserves all the relevant data.

The difficulty of the computations arises since the summation polynomials are computed in the algebraic closure. This problem is dealt in [Gaud09] by using *'Weil Restrictions'*, which helps by relocating the computations to a higher genus curve but on a smaller finite extension. Sub-exponential time algorithms exist for efficient computation on higher genus curves, as presented in [Flynn90]. This was an approach which was successful for many particular cases.

Although, this attack methodology is effective for some cases, but in general, the evaluation of the resultants for the computation of summation polynomials, as mentioned in theorem 1.3.1, is necessary. But, the evaluation of resultants is a computationally heavy task. In the next section, we will provide a novel method named as the **Curve Intersection Method**, which deals with a novel geometric interpretation of EC-DLP, and helps in averting the evaluation of these resultants.

Finally, when an attack was designed, as described in subsection 1.4.2, it did not result in a considerable improvement over the existing methods for a field with large characteristic $p > 500,000$, and their respective algebraic extensions.

1.3.2 Grobner Basis

We have used the concept of a Grobner Basis in the algorithm of intersection method given in Appendix A. In this subsection, we provide the definition and an example of Grobner Basis.

Definition 1.3.3 (*Grobner Basis* [Kobl12])**.** Let, $F = \{g_1, ..., g_l\} \subset \mathbb{F}[X] = \mathbb{F}[X_1, ..., X_m]$ be a finite set of polynomials in m variables over a field $\mathbb{F}$; and let I be the ideal of $\mathbb{F}[X]$ that they generate. We say that F is a Grobner basis for the ideal I, if **every** nonzero polynomial $f \in I$ has leading term that is divisible by the leading term of at least one of the g_i.

Example 1.3.1 ([Kobl12]). Let, $f(X, Y, Z) = X^2Y^2 + XY \in \mathbb{F}[X, Y, Z]$, where $\mathbb{F}$ is any field. Let $F = \{g_1, g_2, g_3\}$, be a basis where, $g_1(X, Y, Z) = Y^2 + Z^2$, $g_2(X, Y, Z) = X^2Y + YZ$, and $g_3(X, Y, Z) = Z^3 + XY$. If we first reduce f modulo g_1 we obtain $-X^2Z^2 + XY$, which cannot be reduced further, because neither of its terms is divisible by the leading terms of g_1, g_2 *or* g_3. On the other hand, if we first reduce f modulo g_2 we obtain $-Y^2Z + XY$, which can be reduced modulo g_1 to get $Z^3 + XY$. Finally, we can reduce the last result modulo g_3. Hence, we see that Grobner Basis provides us with a criterion for making a better choice of basis polynomials.

1.4 Curve Intersection Method

In subsection 1.4.1, we provide the main result on *Intersection of Curves*, after which in subsection 1.4.2, we use theorem 1.4.2 to design an attack on EC-DLP, which is only effective for finite fields having small characteristic $p < 500,000$.

1.4.1 Result on Intersection of Curves

Let, E be an Elliptic Curve over a finite field $\mathbb{F}_p$ of characteristic p, for some prime $p \geq 5$. Let, points P and $Q \in E$ and $n \in \mathbb{Z}/N\mathbb{Z}$, where N is the order of the point P. We can define the EC-DLP in this setting as,

$$Q = nP,$$

where $n < \#E$. By Hasse's Theorem (refer theorem 1.2.1), we have that $\#E \sim p$. The order of P is known, since it can be efficiently computed by the **SEA** algorithm [Scho95]. Let, $m = \lfloor \log_2(N) \rfloor$. Now, we can express n as,

$$n = \sum_{i=0}^{m} \epsilon_i 2^i \qquad\qquad \epsilon_i \in \{0, 1\},$$

Then, we define P_i as,

$$P_i := 2^i P \qquad \forall i = 0, ..., m.$$

It follows that,

$$Q = \sum_{i=0}^{m} \epsilon_i P_i.$$

Let, $K(E)$ be the set of all rational functions. Note that if we are able to find a function $f \in K(E)$ such that the support of $div(f)$ is contained in $\{P_0, ..., P_m, -Q, \mathcal{O}\}$, then we will be able to find a relation among P and Q. This is the central concept of our geometric approach for solving the EC-DLP. To illustrate this fact we provide a well known theorem from basic algebraic geometry.

Theorem 1.4.1 ([ShRe94]). *Let X be an affine variety. Then a rational function which is regular at all points of X can be described as a polynomial function.*

Remark 1.4.1. In the theorem above, the rational function is defined on the affine variety. Standard definitions of a rational function, and regular map defined over affine varieties is used. For a detailed exposition, one can refer to [ShRe94, Section 1.4 and 2.3].

Definition 1.4.1 (Valuation [Ful08]). Let, $h(x)$, $g(x)$, and $p(x)$ be polynomials defined over a field $\mathbb{K}$; such that $g(x)$ divides $h(x)$, and $g(x)$ does not divide $p(x)$. Let, ϕ be a positive integer. If we can express,

$$h(x) = (g(x))^{\phi} * p(x).$$

The valuation is then defined as the 'multiplicity' ϕ, and denoted by,

$$v_{g(x)}(h(x)) = \phi.$$

Now, we prove the *main* result of this chapter. In the following theorem, we prove a relationship between valuation and intersection number. As plane curves intersect at various points and they have multiplicities, hence, *intersection number* plays a key role in identifying them uniquely. An excellent exposition can be found in [Ful08, Chapter 3]. The intersection number of two curves A and B at point Q is denoted by $(A \cdot B)_Q$.

Theorem 1.4.2 (Intersection of Curves). *Let, $E : y^2 - (x^3 + Ax + B)$ be an Elliptic Curve over a finite field $\mathbb{F}_p$ of prime characteristic $p \geq 5$, and $C : f(x, y) = 0$ be an affine curve. Let, $r(x) := Res_y(f(x, y), y^2 - (x^3 + Ax + B))$ be the resultant, and $P_0 = (x_0, y_0) \in E$. Then the valuation is,*

$$v_{(x-x_0)}(r(x)) = (C \cdot E)_{P_0} + (C \cdot E)_{-P_0}.$$

Proof. It is a two step proof.

Step 1: To reduce the claim to the case, in which, there are no points of $C \cap E$ on the same vertical line.

Step 2: Proving that,

$$v_{x-x_0}(r(x)) = (C \cdot E)_{P_0}.$$

□

Proof of Step 1. Considering $\dfrac{f(x,y)}{x-x_0}$ is regular on the affine part of E, there exists a polynomial $g(x,y)$ such that $g(x,y) = \dfrac{f(x,y)}{x-x_0}$ on $E(\overline{\mathbb{F}}_p)$ or equivalently $f(x,y) = (x-x_0)g(x,y) \pmod{E}$ (Invoking Theorem 1.4.1). The resultant is multiplicative and it follows that,

$$Res_y(E, f(x,y)) = Res_y(E, x-x_0)Res_y(E, g(x,y)),$$

$$Res_y(E, f(x,y)) = (x-x_0)^2 Res_y(E, g(x,y)).$$

Iterating the process we get the reduction which proves our assertion for the first step. □

Proof of Step 2. In step 1, we have proved that there are no points of intersection of C and E on the same vertical line. Hence, our assertion becomes,

$$v_{x-x_0}(r(x)) = (C \cdot E)_{P_0}.$$

We observe that if all the points are simple then the *resultant* is a square-free polynomial which is given by,

$$\prod_{P(x_P,y_P) \in C \cap E} (x - x_P).$$

Let's consider the case, in which, we have a tangent T_{P_0} at P_0, then,

$$v_{x-x_0} = Res_y(E, T_{P_0}) = 2 \text{ or } 3.$$

This depends if any point P is a *flex* or not. We prove the step 2 by induction on,

$$M = \sum_{P(x_P,y_P) \in C \cap E} (x - x_P)(C \cdot E)_P - 1.$$

If, $M = 0$ then the points are simple. Let's suppose that $M > 0$, and let P_0 be a point such that the $(C \cdot E)_{P_0} \geq 2$. Then, considering $\dfrac{f(x,y)}{T_{P_0}}$ we have the following three possibilities.

(1) Considering P_0 is not a flex. If, all the points of intersection belong to $C \cap E$, and P_0 is not a flex. Then, $\dfrac{f(x,y)}{T_{P_0}}$ is a regular function. Hence, by the previous argument, we can reduce M and apply induction accordingly to deduce the result.

(2) If, P_0 is not a flex, but we have a third point of intersection $R \notin C \cap E$. Then, considering a line L_R passing through R and through other two points whose x-coordinates are different from each other, and also different from that of the points in $C \cap E$, we deduce that $\left(\dfrac{f(x,y)}{T_{P_0}}\right)(L_R)$ is regular, and the value of M for the divisor associated to this function has been reduced.

(3) If P_0 is a flex. Then, we have two sub-cases.

3(a) $\qquad (C \cdot E)_{P_0} \geq 3.$

In this case, it is a straightforward deduction that $\dfrac{f(x,y)}{T_{P_0}}$ is regular in the affine part of E, and in this way we have reduced the value of M, and apply induction accordingly to deduce the result.

3(b) $\qquad (C \cdot E)_{P_0} = 2$

For this case we consider a line passing through P_0 and other two points whose x-coordinates are different from each other, and also different from that of the points in $C \cap E$. Now, we deduce that $\left(\dfrac{f(x,y)}{T_{P_0}}\right)(L_{P_0})$ is regular, and the value of M for the divisor associated to this function has reduced. This substantiates our claim. □

Now, we apply this and continue with the explanation of the intersection method in the perspective of designing an attack on EC-DLP.

1.4.2 Intersection of Curves and Elliptic Curve Discrete Logarithm Problem

Let, P be a point on an elliptic curve E over a finite field $\mathbb{F}$, and $\overline{\mathbb{F}}$ be the algebraic closure of $\mathbb{F}$.

Definition 1.4.2 (*Divisors* [Wash03])**.** For each point $P \in E(\overline{\mathbb{F}})$, let's define a formal symbol $[P]$. A divisor D on E is a finite linear combination of such symbols with integer coefficients,

$$D = \sum_i a_i[P_i], \quad a_i \in \mathbb{Z}.$$

Definition 1.4.3 (*Degree of a Divisor* [Wash03])**.**

$$deg(D) = \sum_i a_i$$

Definition 1.4.4 (*Order of Vanishing* [Wash03])**.** Let, f be a rational function. Then, the order of vanishing $ord_P(f)$ of f at point P is defined as the multiplicity of the zero/pole of f at P.

Definition 1.4.5 (*Principal Divisor* [Wash03])**.** The *Divisor* of a non-zero rational function is named as Principal Divisor,

$$div(f) = \sum_{P \in E(\overline{\mathbb{F}})} ord_P(f) \bullet [P].$$

Definition 1.4.6 (*Degree* 0 *Picard Group* [Wash03])**.**

$$Pic^0(E) = \{Degree\ 0\ Divisors\ on\ E\}/\{Principal\ Divisor\ on\ E\}.$$

Let's denote the degree zero Divisors of the elliptic curve E by $Div^0(E)$. We can define a sum map σ: $Div^0(E) \to E(\overline{\mathbb{F}})$, given by $\sigma(\sum_i a_i[P_i]) = \sum_i a_i P_i$, which is a homomorphism. It is surjective because $\sigma([P] - [O]) = P$, where O is the point at infinity. This sum map provides us with the isomorphism between the Picard group and the elliptic curve.

Suppose that the solution n to the EC-DLP is even and let,

$$\frac{n}{2} = \sum_{i=0}^{m-1} \varepsilon_i \cdot 2^i.$$

This is the base two decomposition. Note that this is not a huge restriction, as we can check for $P = (n-1)Q$, in case we do not find an even n. Now, we recall the group isomorphim,

$$E \to Pic^0(E),$$

$$P \mapsto [P] - [O].$$

Here, we want to highlight that in $Pic^0(E)$, we can view the EC-DLP in terms of divisors. The idea here is to use the concept of principal divisors which enables us to write the relations of the following form,

$$\sum_i P_i = O.$$

Hence, we can be sure that we can write these relationships in terms of polynomial functions $f(x, y)$ on E such that the $div(f) = \sum_i [P_i] - [O]$ in the group of divisors. This implies that the restriction to the affine part of E is equal to $\sum_i [P_i]$. Since, $n = \sum_{i=0}^{m-1} 2\varepsilon_i \cdot 2^i$. We can conclude that there exists a function $f(x, y) \in K(E)$ which is regular in the affine part of E, such that,

$$div(f) = (-2m-1)[O] + [-Q] + \sum_{i=0}^{m-1} (1+\varepsilon_i)[P_i] + (1-\varepsilon_i)[-P_i].$$

Note that, by theorem 1.4.2 on intersection of curves we have that,

$$Res_y(f(x,y), y^2 - (x^3 + Ax + B)) = (x - x_0)^2 \cdots (x - x_{m-1})^2 (x - x_Q),$$

where $P_i = (x_i, y_i)$ and $Q = (x_Q, -y_Q)$. Since, f is regular in the affine part of E, so it is an element of $\mathbb{F}_p[x, y]/(y^2 - (x^3 + Ax + B))$, which is uniquely determined by a polynomial of the form,

$$f(x, y) = yg(x) + h(x).$$

Let, $d = \deg(f(x, y))$, now we can express,

$$g(x) = g_0 + ... + g_{d-1}x^{d-1},$$

and

$$h(x) = h_0 + ... + h_d x^d.$$

Hence, the functions which are regular on the affine part can be parametrized up to constant on a projective space of dimension $2d$. The resultant can be expressed (up to multiplication by a non-zero constant) in the following way,

$$r(x) = (h(x))^2 - (g(x))^2(x^3 + Ax + B).$$

Hence, if $g_{d-1} \neq 0$ and $r(x)$ is an univariate polynomial of degree $2d + 1$; It follows that imposing $d = m$ and $g_{d-1} = 1$, we get,

$$r(x) = (x - x_0)^2 \cdots (x - x_{m-1})^2(x - x_Q).$$

Remark 1.4.2. We are imposing the condition that, $2m+1 = 2d+1$ on an affine space of dimension $2m$.

Let, $I \triangleleft \kappa[g_0, ..., g_{d-2}, h_0, ..., h_d]$ be the ideal generated by these equations. This results in an over-determined system. The Diffie-Helmann Key exchange which is the basic example of posing EC-DLP would not be possible if there is no solution to this over-determined system. Hence, it can be safely assumed that for such a system for specific/recommended curves (used for cryptography) will have solution. But if there is a solution, then there are at least **two**. As a matter of fact,

$$(g_0, ..., g_{d-2}, h_0, ..., h_d) \in V(I) \iff (g_0, ..., g_{d-2}, -h_0, ..., -h_d) \in V(I).$$

This corresponds to the following,

$$Q = \sum_{i=0}^{m-1} [2\varepsilon_i]P_i \iff -Q = \sum_{i=0}^{m-1} [-2\varepsilon_i]P_i.$$

In general, there can be also more solutions, if we do not require that $f(P_i) = 0$ and $f(-Q) = 0$, which are $m + 1 = d + 1$ linear conditions on the coefficients of f. So, at the end we have a variety characterized by $d + 1$ linear equations and $2d + 1$ quadratic equations. Note that some of the quadratic conditions are redundant. One of the instances is the condition $f(x_i, y_i) = 0$ and $r(x_Q) = 0$ which imply that $r(x_i) = 0$ and $r(x_Q) = 0$. Therefore, there are $d + 1$ linear conditions

and d independent quadratic conditions given by,

$$r'(x_i) = 0, \qquad \forall\ i\ \in\ \{0, ..., m-1\}.$$

Thus, essentially we are studying the zero set of the interesection of d quadric hypersurfaces in an affine space of dimension $d-1$.

Remark 1.4.3. Note that if the order of the point P is even and n is odd, then this method produces *no solution*. Instead, if n is even, then there can be two solutions, if n added to the order of point P; have the same binary length as the order of point P. If order of point P is odd, then there is a unique solution, provided n is even. If n is *odd*, there is exactly one solution corresponding to the addition of n with order of point P.

1.5 Conclusion and Future Work

The dimension of the system of equations that needs to be solved for the implementation of the attack described in subsection 1.4.2 depends on the number of points in $E(\mathbb{F}_p)$. Typically, the efficiency of the curve intersection method depends on how large is the characteristic of the underlying field. In conclusion, we can only claim that our method is useful for elliptic curves over finite fields of small characteristic (primes greater than 4 and less than $500,000$).

If we consider implementation of the Curve Intersection Method for $E(\mathbb{F}_{p^n});\ (n > 1)$, then we have to solve a large over-determined system of equations, which is *not* suitable for designing real-time attacks. The algorithm given in Appendix A, works well for smaller extensions. A typical experiment shows that, if we consider $p = 5$, then we can devise an attack upto the 9^{th} extension; $(n \leq 9)$, beyond which the time taken for solving the system of equations is not practical.

The complexity of the curve intersection algorithm depends majorly on finding the vanishing ideals and solutions of the system of equations which are over-determined, which are hard to solve (and might have exponential complexity in many cases). Some machine learning techniques gives us hope to solve these kind of systems in a comparatively lower (probabilistic) time complexity. Another approach which is worth exploring is Zhuang-Zi [DiGS06], which provides a new technique to solve system of multivariate polynomial equations over a finite field.

Chapter 2

Odd Recursive Towers

Note 2.0.1. This chapter entails the results from the research paper titled *High Order Elements in Finite Fields Arising from Recursive Towers* by Valerio Dose, Pietro Mercuri, Ankan Pal (the PhD candidate), Claudio Stirpe. To read the full reference disclaimer, please refer to [0.1].

2.1 Chapter Description

Abstract. In [$BCGH^+09$], some recursive equations of a tower of fields corresponding to modular curves were used to produce high multiplicative order elements in finite field extensions. In this research work, we use purely algebraic conditions to find several towers of fields producing high order elements in GF$(p, 2^n)$, for odd p, for $n \geq 1$. Such towers are given recursively in the form $x_n^2 + x_n = v(x_{n-1})$, for odd p, where $v(x)$ is a polynomial of small degree over the prime field GF$(p, 1)$ and x_n belongs to the finite field extension GF$(p, 2^n)$, for p odd. The lower bounds of the orders of the groups generated by x_n, or by the discriminant δ_n of the polynomial, are similar to [$BCGH^+09$].

In this chapter, we will illustrate the concept of *Recursive Tower* in section 2.3 and how it can be used to construct high order elements in extensions of finite fields. In this research work, we found some bivariate polynomial equations which can be used for constructing high order elements in finite field extensions. We could produce an element whose order was larger than 2^{1771}, under 650 seconds. The idea was to change the polynomials into a recursive form and then utilize this relationship to produce high order elements in the finite field extensions. This chapter starts with a *literature survey* of various methods (described in section 2.2) which are used widely for finding (near) primitive elements in finite fields. Using elementary techniques from Algebraic Number Theory, we prove the results about odd recursive towers in subsection 2.3.1.

Note 2.1.1. In this research work, we also delve into even recursive towers. But, in the thesis we have not included/discussed the case of even recursive towers.

2.2 High Order Elements in Finite Fields

Finite Fields are a source of many challenging computational problems. A good survey of the algorithmic and computational problems can be found in [Shpar12]. Notably, finding irreducible polynomials and solving discrete logarithms, are two problems which have found ample application in Cryptography and Coding Theory. Some associated problems are polynomial factorization, finding bases, and finding primitive elements, which inspires many innovative approaches to problem solving. We will focus primarily on the discrete logarithm problem, which can be posed in the multiplicative group of a finite field. Finding primitive element(s) is one of the basic requirement towards this.

In cryptography, high order elements can give rise to designing safer primitives. Recently, a team at Google achieved Quantum Supremacy [AAB919]. We can safely assume that the post-quantum era is not a far-fetched reality. This has provided impetus to the field of Post-Quantum

Cryptography for producing quantum resistant protocols. Nevertheless, the transitioning stages are as pivotal as post-quantum cryptography. Hence, strengthening the present state of the art cryptographic protocols has become inevitable. Discrete Logarithm Problem is a widely studied cryptographic problem and the easiest way to strengthen it, can be achieved by finding high order elements in a finite field. This motivated us to find new avenues/methods/recipes which can produce high order elements in a finite field. A naive approach to this problem is 'recursion' or recursive relations defined over finite fields and their field extensions. The cardinal motivation of this research work is the question that '*where to find such meaningful recursions*'?

Let, $\mathbb{F}_p$ be a finite field of characteristic p and $\mathbb{F}_p^*$ be the multiplicative group of the finite field. Let, a and b be the elements of $\mathbb{F}_p^*$, where a is a primitive element. We divulge shortly into the complexity of finding a for the discrete logarithm problem ($a^n = b$) in $\mathbb{F}_p^*$. Traditionally, Gauss periods can be efficiently used for finding elements of high order in a Finite Field. Gathen et. al. in [GaSh95], provide computational ways to use this method for producing high order elements.

Definition 2.2.1 (Gauss Period [GGP98])**.** Let, n and k be positive integers such that $s = nk+1$ is a prime, not dividing p (the characteristic of $\mathbb{F}_p$). If H is a subgroup of order k of the multiplicative group of $\mathbb{Z}/s\mathbb{Z}$. For any primitive s^{th} root β of unity in $\mathbb{F}_{p^{nk}}$, the element:

$$\alpha = \sum_{d \in H} \beta^d,$$

is a Gauss period of type (n, k) over $\mathbb{F}_p$.

Finding elements of high multiplicative order in a finite field is an interesting problem in computational number theory and finds applications in cryptology (for instance, Discrete Logarithm Problem). A generic method was given in [Gao99], later improved in [Con01], and [Popov14A]. Other strategies which allow to construct elements of high order usually address specific sequences in finite fields. In this regard, the methods involving Gauss periods are summarized in [GaSh01]. Notably, there is an extensive literature available in [AhSh10], [Popov12], [Popov13], [Chang13], and [Popov14B].

Another interesting approach is to look for high order elements which arise as coordinates of points on an algebraic curve defined over a finite field (refer to [Vol07], [Vol10], and [Chang13]). One way which has been explored for generating elements of this type is through the iterative use of polynomial equations of type $f(x_{n-1}, x_n) = 0$, defining suitable towers of fields, which we address as *recursive towers* in this research work. Similar examples can be found in [BCGH+09], [Vol10], [Popov15A], and [Popov18].

2.3 High Order Elements in Finite Fields arising from Odd Recursive Towers

2.3.1 Towers in Odd Characteristic

Let p be an odd prime. Let $k \in \mathbb{Z}$ be a non-negative integer, by $\mathrm{GF}(p, 2^k)$, we will denote a field having p^{2^k} elements. By tower of fields, or simply a tower, we mean a sequence of field extensions,

$$K_1 \subset K_2 \subset \ldots \subset K_n \subset \ldots$$

All the towers we consider are *finite, normal and separable*, i.e., each extension K_n/K_{n-1} is finite, normal, and separable, for every $n > 1$. For each positive integer n, let the extension $K_n = \mathrm{GF}(p, 1)[x_n]$, where the element $x_n \in \mathrm{GF}(p, 2^n)$ is given by a recursive formula $f(x_{n-1}, x_n) = 0$, for a polynomial $f(x, y) \in \mathrm{GF}(p, 1)[x, y]$. In this case, we say that the tower $K_1 \subset K_2 \subset \ldots \subset K_n \subset \ldots$ is defined by $f(x_{n-1}, x_n)$, and we address this kind of towers as recursive towers. We focus on towers defined by $f(x_{n-1}, x_n) = x_n^2 + x_n - v(x_{n-1})$, for $n \geq 2$, with $x_1 \in \mathrm{GF}(p, 2)$, and where $v(x)$ is a polynomial in $\mathrm{GF}(p, 1)[x]$. We denote by δ_n the discriminant $\delta_n = 1 + 4v(x_n)$, for $n \geq 1$. We point out that both elements x_n and δ_n belong to $\mathrm{GF}(p, 2^n)$, but they could also lie in a smaller extension $\mathrm{GF}(p, 2^m)$ for some $m < n$. Given the tower defined by $f(x_{n-1}, x_n)$, we denote by $g(x, y) \in \mathrm{GF}(p, 1)[x, y]$ a polynomial giving the relation between two consecutive discriminants δ_{n-1} and δ_n, namely $g(\delta_{n-1}, \delta_n) = 0$.

Note 2.3.1 (Uniqueness). There can exist multiple polynomials $v(x_n)$, which can produce the same tower. We only provide some of the examples, which were useful in producing high order elements.

We use the following lemma for estimating the order of the elements in finite fields. Burkhart et. al. proved in [BCGH+09, Lemmas 1 and 2] the following lemma using elementary means. The gcd calculation is a consequence of the computation following the Euclid's algorithm. After that, we can check the divisibility of $a^{\ell^b(\ell-j)}$ and $a^{\ell^c(\ell-j)}$ by ℓ, and thus the co-primality argument follows through.

Lemma 2.3.1 ([BCGH+09])**.** Let ℓ be a prime, and let a, b, and c be positive integers such that $b < c$. Assume $a \equiv 1 \bmod \ell$. Let p be a prime dividing $\frac{1}{\ell}\sum_{j=1}^{\ell} a^{\ell^b(\ell-j)}$. Then $p > \ell^{b+1}$ and $\gcd\left(\sum_{j=1}^{\ell} a^{\ell^b(\ell-j)}, \sum_{j=1}^{\ell} a^{\ell^c(\ell-j)}\right) = \ell$. In particular $\frac{1}{\ell}\sum_{j=1}^{\ell} a^{\ell^b(\ell-j)}$ and $\frac{1}{\ell}\sum_{j=1}^{\ell} a^{\ell^c(\ell-j)}$ are coprime.

Remark 2.3.1. Lemma 2.3.1 is true for all p and not only odd prime.

Given two positive integers j and n such that $j < n$, we denote by $\mathrm{N}_{n,j} \colon \mathrm{GF}(p, 2^n) \to \mathrm{GF}(p, 2^{n-j})$ the norm of the field extension $\mathrm{GF}(p, 2^n)/\mathrm{GF}(p, 2^{n-j})$, namely $\mathrm{N}_{n,j}(x) = x^{\prod_{i=1}^{j}(p^{2^{n-i}}+1)}$. We use the

conventions $\mathrm{N}(x) := \mathrm{N}_{n,1}(x)$ and $\mathrm{N}_{n,0}(x) = x$.

Note 2.3.2. By good towers K_n, we will refer to those towers for which high order elements can be constructed through the recursive form of $f(x_n, x_{n-1})$.

In order to find good towers we restrict our search to polynomials $f(x, y) = y^2 + y - v(x)$, with $v(x) \in \mathrm{GF}(p, 1)[x]$ being a non-zero polynomial, which satisfy Condition **(1)** below, and at least one condition out of **(2)** or **(2')**.

(1) $\frac{f(x_{n-1},0)}{x_{n-1}}$ is a square in $\mathrm{GF}(p, 2^{n-1})$ for $n \geq 2$;

(2) $\frac{g(\delta_{n-1},0)}{x_{n-1}}$ is a square in $\mathrm{GF}(p, 2^{n-1})$ for $n \geq 2$;

(2') $\frac{g(\delta_{n-1},0)}{\delta_{n-1}}$ is a square in $\mathrm{GF}(p, 2^{n-1})$ for $n \geq 2$.

Remark 2.3.2. Condition **(2')** above is satisfied by other towers of fields in the literature, see for example [BCGH+09, section 4, formula (5)]. We do not know whether the corresponding tower (see [BCGH+09, section 2, equation (2)]), which does not satisfy Condition **(1)** above, satisfies a suitable analogue of this condition which ensure that Theorem 2.3.1 below holds.

Remark 2.3.3. These conditions are not sufficient for obtaining high order elements from each tower, but, for our particular choice of f, they are sufficient to construct a recursive tower defined by $f(x_{n-1}, x_n)$, as Theorem 2.3.1 below shows.

The following theorem ensures that all the polynomials $f(x_{n-1}, x_n)$ listed in section 2.3.2 define towers of fields. In particular it shows that $[K_n : K_{n-1}] = 2$, for all $n > 1$. The proof is a generalization of the argument given in [BCGH+09, Proposition 1].

Theorem 2.3.1. *Let $v(x) \in \mathrm{GF}(p, 1)[x]$ be a polynomial and assume that $f(x_{n-1}, x_n) = x_n^2 + x_n - v(x_{n-1})$ satisfies Conditions **(1)** and **(2)**, or Conditions **(1)** and **(2')**. If x_{n-1} and δ_{n-1} are not squares in the multiplicative group $\mathrm{GF}(p, 2^{n-1})^*$ for a suitable $n \geq 2$, then x_j and δ_j are not squares in the multiplicative group $\mathrm{GF}(p, 2^j)^*$, for $j \geq n$.*

Proof. The element x_n is not in $\mathrm{GF}(p, 2^{n-1})$ because δ_{n-1} is not a square in $\mathrm{GF}(p, 2^{n-1})$, so $f(x_{n-1}, y)$ is the minimal polynomial of x_n. We need to ensure that $x_n^{(p^{2^n}-1)/2} = -1$. As in [BCGH+09, Proposition 1], we obtain,

$$x_n^{(p^{2^n}-1)/2} = (x_n^{p^{2^{n-1}}+1})^{(p^{2^{n-1}}-1)/2} = \mathrm{N}(x_n)^{(p^{2^{n-1}}-1)/2} =$$
$$= f(x_{n-1}, 0)^{(p^{2^{n-1}}-1)/2} = -1,$$

where $\mathrm{N}(x_n) = x_n^{p^{2^{n-1}}+1} = f(x_{n-1}, 0)$ is the norm of x_n over $\mathrm{GF}(p, 2^{n-1})$, and we use Condition **(1)** in last equality to show that $f(x_{n-1}, 0)$ is not a square in $\mathrm{GF}(p, 2^{n-1})$ for $n > 1$. Consider the

discriminant δ_n. Again $g(\delta_{n-1}, y)$ is the minimal polynomial of $\delta_n = 1 + 4v(x_n)$. Since, in GF$(p, 2^n)$, we know that $\frac{f(x_n,0)}{x_n}$ is a square by Condition **(1)**, -1 is a square and x_n is not a square as above, then $v(x_n) = -f(x_n, 0)$ is not a square in GF$(p, 2^n)$. Hence, $\delta_n \notin$ GF$(p, 2^{n-1})$. The same computation as above yields,

$$\begin{aligned}\delta_n^{(p^{2^n}-1)/2} &= (\delta_n^{p^{2^{n-1}}+1})^{(p^{2^{n-1}}-1)/2} = \mathrm{N}(\delta_n)^{(p^{2^{n-1}}-1)/2} = \\ &= g(\delta_{n-1}, 0)^{(p^{2^{n-1}}-1)/2} = -1,\end{aligned}$$

where we use Condition **(2)**, respectively **(2')**, in last equality to show that $g(\delta_n, 0)$ is not a square in GF$(p, 2^{n-1})$, because x_{n-1}, (respectively δ_{n-1}), is a non-square by hypothesis. It follows that x_n and δ_n are non-squares in GF$(p, 2^n)$. Repeating the same argument, we find that x_j and δ_j are not squares in GF$(p, 2^j)$, for all $j > n$, which completes the proof. □

The importance of this theorem is clear if we consider Corollary 2.3.1 below, which is an analogue of [BCGH+09, Proposition 2]. We first state the following property of the norm that is used in the proof of the corollary.

Lemma 2.3.2. Let $n \geq 2$ and $j < n$ be positive integers, then

$$\frac{\mathrm{N}_{n,j}(x_n)}{x_{n-j}} = \prod_{k=1}^{j} \mathrm{N}_{n-k,j-k}\left(\frac{\mathrm{N}_{n-k+1,1}(x_{n-k+1})}{x_{n-k}}\right).$$

Moreover $\frac{\mathrm{N}_{n,j}(x_n)}{x_{n-j}}$ is a square in GF$(p, 2^{n-j})$.

Proof. The case $j = 1$ is trivial. By induction on j, let $j \geq 2$ and assume the result holds for $j - 1$, then

$$\begin{aligned}\frac{\mathrm{N}_{n,j}(x_n)}{x_{n-j}} &= \frac{x_n^{(p^{2^{n-1}}+1)\prod_{i=2}^{j}(p^{2^{n-i}}+1)}}{x_{n-j}} = \\ &= \left(\frac{x_n^{p^{2^{n-1}}+1}}{x_{n-1}}\right)^{\prod_{i=2}^{j}(p^{2^{n-i}}+1)} \frac{x_{n-1}^{\prod_{i=2}^{j}(p^{2^{n-i}}+1)}}{x_{n-j}} = \\ &= \left(\frac{\mathrm{N}_{n,1}(x_n)}{x_{n-1}}\right)^{\prod_{i=2}^{j}(p^{2^{n-i}}+1)} \frac{\mathrm{N}_{n-1,j-1}(x_{n-1})}{x_{n-j}} = \\ &= \left(\frac{\mathrm{N}_{n,1}(x_n)}{x_{n-1}}\right)^{\prod_{i=1}^{j-1}(p^{2^{n-1-i}}+1)} \prod_{k=1}^{j-1} \mathrm{N}_{n-k-1,j-k-1}\left(\frac{\mathrm{N}_{n-k,1}(x_{n-k})}{x_{n-k-1}}\right) =\end{aligned}$$

$$= \mathrm{N}_{n-1,j-1}\left(\frac{\mathrm{N}_{n,1}(x_n)}{x_{n-1}}\right)\prod_{k=2}^{j}\mathrm{N}_{n-k,j-k}\left(\frac{\mathrm{N}_{n-k+1,1}(x_{n-k+1})}{x_{n-k}}\right).$$

The remaining part of the proof follows by Condition **(1)**. □

Corollary 2.3.1. Let $v(x)$ be a polynomial in $\mathrm{GF}(p,1)[x]$ and assume that $f(x_{n-1},x_n) = x_n^2 + x_n - v(x_{n-1})$ satisfies Conditions **(1)** and **(2)**, or Conditions **(1)** and **(2')**, and that x_1 and δ_1 are not squares in $\mathrm{GF}(p,2)$. Then $x_n^2 \notin \mathrm{GF}(p,2^{n-1})$ and the order of x_n is greater than

$$2^{\frac{1}{2}(n^2+3n)+\mathrm{ord}_2(p-1)-2},$$

for all $n > 1$. The same lower bound also holds for the order of δ_n if $\delta_n^2 \notin \mathrm{GF}(p,2^{n-1})$ for all $n > 1$.

Proof. We know that $x_n \notin \mathrm{GF}(p,2^{n-1})$ by Theorem 2.3.1, therefore $x_n^2 = -x_n + v(x_{n-1}) \notin \mathrm{GF}(p,2^{n-1})$ for all $n > 1$. We show that the order of x_n has a common factor with the odd number $\frac{p^{2^{n-j}}+1}{2}$ proving that $x_n^{\frac{2(p^{2^n}-1)}{p^{2^{n-j}}+1}} \neq 1$, for $j = 1,2,\ldots,n-1$. For $j = 1$, we have

$$x_n^{\frac{2(p^{2^n}-1)}{p^{2^{n-1}}+1}} = x_n^{2(p^{2^{n-1}}-1)} \neq 1,$$

since $x_n^2 \notin \mathrm{GF}(p,2^{n-1})$, as we have just seen. For $j \geq 2$, we get

$$x_n^{\frac{2(p^{2^n}-1)}{p^{2^{n-j}}+1}} = \left(x_n^{\prod_{k=1}^{j-1}(p^{2^{n-k}}+1)}\right)^{2(p^{2^{n-j}}-1)} = \mathrm{N}_{n,j-1}(x_n)^{2(p^{2^{n-j}}-1)}$$

and the last member above is 1 only if $\mathrm{N}_{n,j-1}(x_n)^2 \in \mathrm{GF}(p,2^{n-j})$. We show that this is not possible. Consider $\mathrm{N}_{n,j}(x_n) = \mathrm{N}_{n-j+1,1}(\mathrm{N}_{n,j-1}(x_n))$. If $\mathrm{N}_{n,j-1}(x_n)^2 \in \mathrm{GF}(p,2^{n-j})$, then either $\mathrm{N}_{n,j}(x_n) = \mathrm{N}_{n,j-1}(x_n)^2$ or $\mathrm{N}_{n,j}(x_n) = \mathrm{N}_{n,j-1}(x_n)$. The latter equality is not possible since $\mathrm{N}_{n,j-1}(x_n)$ is not a square in $\mathrm{GF}(p,2^{n-j+1})$ by Lemma 2.3.2 but $\mathrm{N}_{n,j}(x_n) \in \mathrm{GF}(p,2^{n-j})$ is a square in $\mathrm{GF}(p,2^{n-j+1})$. The former equality, by Lemma 2.3.2, gives,

$$1 = \frac{x_{n-j}\prod_{k=1}^{j}\mathrm{N}_{n-k,j-k}\left(\frac{\mathrm{N}_{n-k+1,1}(x_{n-k+1})}{x_{n-k}}\right)}{x_{n-j+1}^2\prod_{k=1}^{j-1}\left(\mathrm{N}_{n-k,j-k-1}\left(\frac{\mathrm{N}_{n-k+1,1}(x_{n-k+1})}{x_{n-k}}\right)\right)^2} =$$

$$= \frac{x_{n-j}\frac{\mathrm{N}_{n-j+1,1}(x_{n-j+1})}{x_{n-j}}\prod_{k=1}^{j-1}\mathrm{N}_{n-k,j-k}\left(\frac{\mathrm{N}_{n-k+1,1}(x_{n-k+1})}{x_{n-k}}\right)}{x_{n-j+1}^2\prod_{k=1}^{j-1}\left(\mathrm{N}_{n-k,j-k-1}\left(\frac{\mathrm{N}_{n-k+1,1}(x_{n-k+1})}{x_{n-k}}\right)\right)^2} =$$

$$= \frac{\mathrm{N}_{n-j+1,1}(x_{n-j+1}) \prod_{k=1}^{j-1} \mathrm{N}_{n-j+1,1}\left(\mathrm{N}_{n-k,j-k-1}\left(\frac{\mathrm{N}_{n-k+1,1}(x_{n-k+1})}{x_{n-k}}\right)\right)}{x_{n-j+1}^2 \prod_{k=1}^{j-1} \left(\mathrm{N}_{n-k,j-k-1}\left(\frac{\mathrm{N}_{n-k+1,1}(x_{n-k+1})}{x_{n-k}}\right)\right)^2} =$$

$$= \frac{(x_{n-j+1})^{p^{2^{n-j}}+1} \prod_{k=1}^{j-1} \left(\mathrm{N}_{n-k,j-k-1}\left(\frac{\mathrm{N}_{n-k+1,1}(x_{n-k+1})}{x_{n-k}}\right)\right)^{p^{2^{n-j}}+1}}{x_{n-j+1}^2 \prod_{k=1}^{j-1} \left(\mathrm{N}_{n-k,j-k-1}\left(\frac{\mathrm{N}_{n-k+1,1}(x_{n-k+1})}{x_{n-k}}\right)\right)^2} =$$

$$= x_{n-j+1}^{p^{2^{n-j}}-1} \prod_{k=1}^{j-1} \left(\mathrm{N}_{n-k,j-k-1}\left(\frac{\mathrm{N}_{n-k+1,1}(x_{n-k+1})}{x_{n-k}}\right)\right)^{p^{2^{n-j}}-1}.$$

Since the last term is 1, then

$$x_{n-j+1} \prod_{k=1}^{j-1} \mathrm{N}_{n-k,j-k-1}\left(\frac{\mathrm{N}_{n-k+1,1}(x_{n-k+1})}{x_{n-k}}\right) \in \mathrm{GF}(p, 2^{n-j}),$$

but this is impossible because x_{n-j+1} is a non-square in $\mathrm{GF}(p, 2^{n-j+1})$, by Theorem 2.3.1, but

$$\mathrm{N}_{n-k,j-k-1}\left(\frac{\mathrm{N}_{n-k+1,1}(x_{n-k+1})}{x_{n-k}}\right) = \mathrm{N}_{n-k,j-k-1}\left(\frac{f(x_{n-k},0)}{x_{n-k}}\right)$$

is a square in $\mathrm{GF}(p, 2^{n-j+1})$, for each $k < j$, by Condition **(1)** and by multiplicativity of the norm.

This odd common factor ensures, by Lemma 2.3.1 with $a = p$, $b = n - j$ and $\ell = 2$, the existence of a lower bound on the order of x_n, namely $p_j > 2^{n-j+1}$, for every $j = 1, 2, \ldots, n-1$. Hence, the order is bounded below by

$$2^{\frac{n(n+1)}{2}-1} = \prod_{j=1}^{n-1} 2^{n-j+1} < \prod_{j=1}^{n-1} p_j.$$

The remaining term $2^{n+\mathrm{ord}_2(p-1)-1}$ follows as in [BCGH+09, Proposition 2]. By the repetition of the difference of squares formula, we get,

$$\mathrm{ord}_2\left(\frac{p^{2^n}-1}{2}\right) = \sum_{j=0}^{n-1} \mathrm{ord}_2(p^{2^j}+1) + \mathrm{ord}_2(p-1) - 1 = n + \mathrm{ord}_2(p-1) - 1,$$

for all $n \geq 1$. It follows that $2^{n+\mathrm{ord}_2(p-1)-1}$ divides the order of x_n because $x_n^{\frac{p^{2^n}-1}{2}} = -1$ by Theorem 2.3.1. The proof for δ_n is similar. □

2.3.2 Examples of Towers in Odd Characteristic

In this subsection we find high order elements in GF$(p, 2^n)$, for odd prime p, using five good towers. In this subsection, we denote by ε the element 4^{-1} inside GF$(p, 1)$. We consider the polynomials $f_i(x_{n-1}, x_n) := x_n^2 + x_n - v_i(x_{n-1})$, for $i \in \{1, 2, \ldots, 5\}$, where $v_i(x)$ is a polynomial chosen as follows.

1. $v_1(x) := \varepsilon x$;
2. $v_2(x) := 4x(x + 3\varepsilon)^2$;
3. $v_3(x) := 2\varepsilon x$;
4. $v_4(x) := 8x(2x + 3\varepsilon)^2$;
5. $v_5(x) := 8x(x + 3\varepsilon)^2$.

Remark 2.3.4. Condition **(1)** holds for all the previous polynomials and the relation between two consecutive discriminants is given respectively by,

$$\begin{aligned}
g_1(\delta_{n-1}, \delta_n) &= \delta_n^2 - \delta_n - \varepsilon\delta_{n-1} + \varepsilon;\\
g_2(\delta_{n-1}, \delta_n) &= \delta_n^2 - \delta_n - 4\delta_{n-1}^3 + 6\delta_{n-1}^2 - 9\varepsilon\delta_{n-1} + \varepsilon;\\
g_3(\delta_{n-1}, \delta_n) &= \delta_n^2 - \delta_{n-1};\\
g_4(\delta_{n-1}, \delta_n) &= \delta_n^2 + 48\delta_{n-1}\delta_n - 256\delta_{n-1}^3 + 288\delta_{n-1}^2 - 81\delta_{n-1};\\
g_5(\delta_{n-1}, \delta_n) &= \delta_n^2 - 16\delta_{n-1}^3 + 24\delta_{n-1}^2 - 9\delta_{n-1}.
\end{aligned}$$

The first two towers satisfy Condition **(2)**. In fact,

$$\begin{aligned}
g_1(\delta_{n-1}, 0) &= -\varepsilon(1 + 4x_{n-1}) + \varepsilon = -x_{n-1};\\
g_2(\delta_{n-1}, 0) &= x_{n-1}(x_{n-1} + 3\varepsilon)^2(x_{n-1}^3 + 6x_{n-1}^2 + 9\varepsilon^2 x_{n-1} + 3\varepsilon^3)^2.
\end{aligned}$$

Similarly the last three towers satisfy Condition **(2')**. In fact,

$$\begin{aligned}
g_3(\delta_n, 0) &= -\delta_n;\\
g_4(\delta_n, 0) &= -256\delta_n(\delta_n - 9\varepsilon^2)^2;\\
g_5(\delta_n, 0) &= -16\delta_n(\delta_n - 3\varepsilon)^2.
\end{aligned}$$

Hence, Theorem 2.3.1 applies to $f_i(x_{n-1}, x_n)$, for $i \in \{1, 2, \ldots, 5\}$ once we have some starting points.

The next two lemmas ensures the existence of a non-square x_1 such that δ_1 is a non-square in GF$(p, 2)$ as well. This would be an analogue of [BCGH+09, Lemma 3]. The major difference is

that, in [BCGH+09] only δ_1 is required to be a non-square and x_1 was unconstrained. Here, we need that *both* must be non-squares. But in [BCGH+09] there is no lower bound for x_n, instead in the present work we have it. The present proof relies mainly on elementary combinatorial arguments.

Lemma 2.3.3. Let $c \in \mathrm{GF}(p,1)$ be a non-zero element. There is at least a non-square $x_1 \in \mathrm{GF}(p,2)$ such that $x_1 + c$ is a non-square as well.

Proof. Consider the action ρ of $\mathrm{GF}(p,1)$ on $\mathrm{GF}(p,2)$ as an additive group, namely $\rho_d(x) = x + d$, for $d \in \mathrm{GF}(p,1)$ and $x \in \mathrm{GF}(p,2)$. Then, $\mathrm{GF}(p,2)$ is partitioned into p orbits. There are exactly $\frac{1}{2}(p^2+1)$ squares in $\mathrm{GF}(p,2)$. Among these, there are all the elements of the orbit $\mathrm{GF}(p,1)$. It follows that there are exactly $\frac{1}{2}(p^2-2p+1)$ square elements in $p-1$ orbits. Hence, there is at least one orbit with at most $\frac{1}{2}(p-1)$ square elements and at least $\frac{1}{2}(p+1)$ non-square elements. We denote this orbit by S. It follows that there are at least two consecutive non-squares in S under the repeated action of ρ_c, namely a and $\rho_c(a) = a + c$. The lemma follows by choosing $a = x_1$. □

Example 2.3.1. Consider, $p = 3$ and $c = 1$. Denote by z a generator of $\mathrm{GF}(3,2)^*$ satisfying $z^2 = z + 1$. There are exactly 5 squares in $\mathrm{GF}(3,2)^*$, but 3 of them are in the same orbit $\mathrm{GF}(3,1)$. The remaining ones are $z^2 = z + 1$ and $z^6 = 2z + 2$. One can check that they belong to the orbits $S_1 = \{z; \quad z+1 = z^2; \quad z+2 = z^7\}$ and $S_2 = \{2z = z^5; \quad 2z+1 = z^3; \quad 2z+2 = z^6\}$. As x_1 we can choose the element $2z$ or $z + 2$. They are both roots of the polynomial $x^2 = 2x + 1$, so we use this polynomial for $p = 3$ in Table 2 of Appendix C.

In order to show the existence of a suitable initial element x_1 for the tower defined by $f_5(x_{n-1}, x_n)$, we prove the following lemma.

Lemma 2.3.4. Let p be an odd prime and let $h(x)$ be a cubic polynomial in $\mathrm{GF}(p,1)[x]$ without multiple roots, such that $h(0) \neq 0$. Then,

(i) The curve $C_1 : y^2 = h(x)$ has at most $p^2 + 2p$ affine $\mathrm{GF}(p,2)$-rational points and the curve $C_2 : y^2 = h(x^2)$ has at least $p^2 - 4p - 1$ affine $\mathrm{GF}(p,2)$-rational points.

(ii) If $p \geq 11$, then there is at least a non-square $x_1 \in \mathrm{GF}(p,2)$ such that $h(x_1)$ is a non-square in $\mathrm{GF}(p,2)$ as well.

Proof. (i). We observe that $h(x^2)$ is square-free since $h(x)$ is square-free and $h(0) \neq 0$ by hypothesis. The first statement follows by Weil bound $|N - (p^2+1)| \leq 2gp$, for every smooth projective curve of genus g with N points over $\mathrm{GF}(p,2)$, since C_1 is an elliptic curve and C_2 is a genus two curve, refer to [Sti09, Propositions 6.1.3 (a) and 6.2.3 (b)]. It is well known that the number of points at infinity is one in an elliptic curve and it is at most two in a genus two curve. Hence, (i) is proved.

(ii). By contradiction we assume that $h(\alpha)$ is a square for all non-square $\alpha \in \mathrm{GF}(p,2)$. Let $\beta \in \mathrm{GF}(p,2)$ be a square root of $h(\alpha)$. Since there are exactly $\frac{1}{2}(p^2-1)$ non-squares in $\mathrm{GF}(p,2)$ and $\beta \neq 0$, except at most for 3 choices of α, then the pairs (α,β) and $(\alpha,-\beta)$ produce at least p^2-4 distinct points of C_1. We show that such points are too many. We estimate the number of squares α such that $h(\alpha)$ is also a square in $\mathrm{GF}(p,2)$. Each point (t,y) in C_2 corresponds to the point (x,y) in C_1 with $x=t^2$. This correspondence is not $1-1$ because, when $t \neq 0$, the point $(-t,y)$ determines the same point in C_1. Let N be the number of affine $\mathrm{GF}(p,2)$-rational points of C_2, then C_1 must have more than $\frac{N}{2}$ affine $\mathrm{GF}(p,2)$-rational points (x,y) with x being a square in $\mathrm{GF}(p,2)$. By Part (i), we have $N \geq p^2-4p-1$. Counting the points of C_1 we get, again by Part (i), $p^2-4+\frac{1}{2}(p^2-4p-1) \leq p^2+2p$ which yields, after a straightforward computation, $p^2-8p-9 \leq 0$. It follows that $p \leq 9$, which is contrary to our assumption on p. Hence, there is at least one non-square $x_1 \in \mathrm{GF}(p,2)$ such that $h(x_1)$ is a non-square too. □

Remark 2.3.5. For suitable polynomials $h(x)$, Part (ii) of the previous lemma also holds for odd primes $p < 11$. Consequently, we are interested in

$$\begin{aligned} h(x) = 1 + 4\, v_5(x) = 1 + 32\, x\, (x+3\varepsilon)^2 = 32\left(x+\frac{1}{2}\right)\left(x^2+x+\frac{1}{16}\right) = \\ = 32\, \left(x+\frac{1}{2}\right)\, \left(x+\frac{1}{2}-a\right)\left(x+\frac{1}{2}+a\right), \end{aligned}$$

where a is a square root of $\frac{3}{16}$ in $\mathrm{GF}(p,2)$. We are interested in this polynomial because $\delta_1 = h(x_1)$, for f_5, so we need that both x_1 and δ_1 are non-squares. It follows that $h(x)$ is square-free for $p=5$ and $p=7$. For $p=5$, if we choose x_1 being a root of the polynomial x^2+4x+2, then $h(x_1)=x_1^5$. Hence, both x_1 and $h(x_1)$ are non-square in $\mathrm{GF}(5,2)$. Similarly, for $p=7$, if we choose x_1 as a root of x^2+5x+5, then both x_1 and $h(x_1)$ are non-squares in $\mathrm{GF}(7,2)$. Finally, for $p=3$, we have that $h(x)$ has multiple roots, but Part (ii) of Lemma 2.3.4 still holds. In fact, if we choose x_1 as a root of the polynomial x^2+2x+2, as in Example 2.3.1, then $h(x_1)=x_1$, hence $h(x_1)$ is a non-square as well. Kindly refer to Remark 2.3.6 for further explanations. We use the aforementioned examples in Table 6 of Appendix C.

The following corollary ensures the existence of towers defined by $f_i(x_{n-1},x_n)$ generating high order elements for $i \in \{1,2,\ldots,5\}$.

Corollary 2.3.2. The polynomials $f_i(x_{n-1},x_n)$, for $i \in \{1,2,\ldots,5\}$, define infinite towers of fields. Moreover, for a suitable choice of x_1, the order of x_n in $\mathrm{GF}(p,2^n)$ is greater than $2^{\frac{1}{2}(n^2+3n)+\mathrm{ord}_2(p-1)-2}$. The same bound holds for δ_n in the towers defined by $f_1(x_{n-1},x_n)$ and $f_2(x_{n-1},x_n)$ and, when $p>3$, for δ_n in the tower defined by $f_4(x_{n-1},x_n)$.

Proof. First, for each tower considered, we show the existence of a non-square starting point x_1 such that the discriminant δ_1 is a non-square as well. A straightforward computation shows that

$\delta_1 = x_1 + 1$ for f_1 and that $\delta_1 = 16x_1^3 + 24x_1^2 + 9x_1 + 1 = (x_1 + 1)(4x_1 + 1)^2$ for f_2. Hence, for the first two polynomials, it is enough to choose x_1 as in Lemma 2.3.3 with $c = 1$. A straightforward computation also shows that $\delta_1 = 2\left(x_1 + \frac{1}{2}\right)$ for f_3 and that $\delta_1 = 128\left(x_1 + \frac{1}{2}\right)(x_1 + 2\varepsilon^2)^2$ for f_4. Hence, for the third and the fourth polynomial, it is enough to choose x_1 as in Lemma 2.3.3 with $c = \frac{1}{2}$. For the last tower, by Remark 2.3.5, we can take x_1 as in Remark 2.3.5 for $p \leq 7$ and we can take x_1 as in Lemma 2.3.4 for $p \geq 11$.

Now, we know, by Remark 2.3.4, that all the considered towers satisfy Conditions **(1)** and **(2)**, or Conditions **(1)** and **(2')**. Therefore, the result for x_n follows by Corollary 2.3.1. For δ_n we have to check that $\delta_n^2 \notin \mathrm{GF}(p, 2^{n-1})$ for $n > 1$, in the tower defined by $f_1(x_{n-1}, x_n)$ and $f_2(x_{n-1}, x_n)$, for $p \geq 3$, and by $f_4(x_{n-1}, x_n)$ for $p > 3$. But this follows by the expression of $g_1(\delta_{n-1}, \delta_n)$, $g_2(\delta_{n-1}, \delta_n)$ and $g_4(\delta_{n-1}, \delta_n)$ in Remark 2.3.4. □

As in [BCGH+09], the bound of the previous corollary does not seem to be sharp, in fact in many cases we were able to construct generators of the multiplicative group $\mathrm{GF}(p, 2^n)^*$, whose order is $p^{2^n} - 1$, which is much higher than $2^{\frac{n^2}{2}}$. The interested reader can compare the tables in Appendix C with the computational results of [BCGH+09].

Remark 2.3.6. The bound in the Corollary 2.3.2 above, does not hold for δ_n in the tower defined by $f_3(x_{n-1}, x_n)$ and $f_5(x_{n-1}, x_n)$. In fact, $\delta_n^2 \in \mathrm{GF}(p, 2^{n-1})$, for all $n > 1$, which can be verified easily. The interested reader can observe this in Table 4 and 6 of Appendix C. A careful comparison between these two tables reveals an interesting difference when $p > 3$. In fact, the order of the discriminant δ_n turns out to grow very slowly in Table 4 in comparison to Table 6. The reason is that in the former tower the discriminants satisfy the relation $g_3(\delta_{n-1}, \delta_n) = \delta_n^2 - \delta_{n-1} = 0$, which yields $\delta_n^{2^{n-1}} = \delta_{n-1}^{2^{n-2}} = \ldots = \delta_1 \in \mathrm{GF}(p, 2)$. This implies that we can estimate the order of δ_n, which turns out to be lower than $2^{n-1+\mathrm{ord}_2(p^2-1)}$. In the tower defined by $f_5(x_{n-1}, x_n)$, we have that $\delta_n^{2^j} \in \mathrm{GF}(p, 2^{n-j})$ holds for $j = 1$, but not for all $j < n$. This explains why the order grows comparatively faster when $p > 3$. In the case $p = 3$ the polynomial equation $g_5(\delta_{n-1}, \delta_n) = \delta_n^2 - \delta_{n-1}^3 = 0$ gives $\delta_n^{2^{n-1}} = \delta_1^{3^{n-1}} \in \mathrm{GF}(3, 2)$. This explains why the numerical results for the order of δ_n are similar to the tower defined by $f_3(x_{n-1}, x_n)$.

Remark 2.3.7. From the relation $g_4(\delta_{n-1}, \delta_n) = 0$ between δ_n and δ_{n-1} in the fourth tower, for $p = 3$, we get $g_4(\delta_{n-1}, \delta_n) = \delta_n^2 - \delta_{n-1}^3 = 0$. Hence, we observe that the proof of last corollary does not work when $p = 3$. We also point out that $f_4(x_{n-1}, x_n) = f_5(x_{n-1}, x_n)$ when $p = 3$. This fact explains why the numerical results in Tables 5 and 6 of Appendix C have the same values in the first two columns.

Of course, there could exist other towers satisfying analogues of Conditions **(1)** and **(2)** or Conditions **(1)** and **(2')** above. An extensive computer search could show the non-existence of similar examples of the form $f(x_{n-1}, x_n) = x_n^2 + x_n + v(x_{n-1})$, with $\deg(v(x)) \leq 3$, at least for small prime fields.

2.4 Comparative Study

One of the primary research question that is explored in our work is, *'does there exist a general recipe to find polynomials which generate high order elements, recursively?'* This is a research theme which is explored by many researchers from days of yore. In the previous sections, a recursive construction was described. At this juncture, it is almost imperative that we justify the utility of this kind of recursive constructions. Also, some pertinent questions being - *'how does our construction enrich the existing literature'* and, *'is our construction consistent with the previous constructions mentioned in the literature'*.

A notable mention, is SD Cohen's model in [Cohen92]. In this research work, Cohen explores an iterated presentation of $GF(p, 2^n)$, for $p \equiv 3 \ (mod\ 4)$ and $p \equiv 1 \ (mod\ 4)$. Comparing our results with [Cohen92, Theorem 8], which deals with $p \equiv 1 \ (mod\ 4)$ case, we arrive at the conclusion (by explicit computation) that it gives similar results as mentioned in the tables of Appendix C. Now, if we compare the results of Cohen's model for $p \equiv 3 \ (mod\ 4)$ from [Cohen92, Theorem 6], then our construction mechanism would produce elements with higher orders. To illustrate the comparison, let's consider a quintessential example of $p = 11$. In the ninth iteration we were able to generate an element of the order 2^{1771}, but by the Cohen's model, one would be able to generate an element of order at most $(120)^*2^9$, which roughly equals to 2^{15}. We tabulate the *comparative study* for $p = 3$, in Table 7 of Appendix C.

In the case of $p \equiv 1 \ (mod\ 4)$, we would like to highlight that although the orders of the elements generated by Cohen's model and our model are similar, but we argue that the choice of polynomials are more in our case. The limited choice of polynomials in Cohen's model (for $p \equiv 1 \ (mod\ 4)$) was ameliorated by Meyn in [Meyn95], by using a transformation of variable $x \rightarrow x + \frac{1}{x}$. It is an interesting research question, that whether our model works under this transformation of variable or not. On a fundamental level the approaches and motives are different. The aim of our research work was to find various recipes for choice of polynomials, whereas Cohen [Cohen92] and Meyn [Meyn95] were interested in an iterative presentation of finite field extensions, which in itself is an interesting research theme, in its own right.

Continuing the comparative study, we again argue that although the orders of the elements that are generated in [$BCGH^+09$], and our work are similar, still the choice of polynomials is limited for [$BCGH^+09$]. If we consider the cryptographic aspect, the greater choice of polynomials in our model, could lead to a successful construction of hierarchical cryptographic protocol of varying security levels in a discrete logarithm problem setting.

An element in $\mathbb{F}_{p^n}$ is said to generate a normal basis over $\mathbb{F}_p$, if its conjugates form a basis of $\mathbb{F}_{p^n}$ as a vector space over $\mathbb{F}_p$. An element generating a normal basis is defined as a normal element [Chap97]. Chapman in [Chap97] provides an interesting model to construct normal elements in a recursive manner. In a recent work of Popovych et. al. [PopSku20] (2020), a lower bound

is provided for the order of normal elements in finite field extension. The lower bound on the order of elements which we derived in Lemma 2.3.1 is higher than the lower bounds given by Popovych et. al. [PopSku20]. In this section, we have provided a comparative study with the relevant literature. In the next section, we provide some concluding remarks for chapter 2.

2.5 Conclusion and Future Work

In [*BCGH*$^+$09], the choice of polynomials for the recursive process to generate high order elements in finite field extensions, was limited to the equations of the modular curve towers in [Elki01]. In this research work, we attempted to generalize the choice of the polynomials. This provides us with more examples with same state of the art results. A central theme of this research work is to find a recipe to choose polynomials for the recursive process. There might be other equations which could help to attain similar bounds. It would be interesting to understand in general which equations are good and which ones are not; for producing high order elements in finite field. We also point out that there could be other explicit towers satisfying similar properties. We were in fact attracted previously by other interesting examples with $v(x)$ being a polynomial of higher degree over GF$(p, 1)$, which turned out to give high order elements, although the proof seems to be much harder. A possible relation linking together these equations could allow to obtain other families of towers with good parameters. We also expect to improve our results by extending the construction of subsection 2.3.1 to higher degree polynomials.

Another question that would be interesting to explore is the possible relation with some geometric construction. In fact, since the tower in [*BCGH*$^+$09] is obtained from the equation of a modular curve, it is a natural question to ask whether the high order results of our towers may be explained by some geometric setting. A better understanding of the subject might also possibly provide a recipe for finding high order elements from towers given in a different form.

Remark 2.5.1 (Complexity). In this chapter, we have used an odd prime p for the construction of towers and proving their subsequent properties. We have given the numerical results for the same in Appendix C. But, the algorithm given in Appendix B can be generalized for any **prime power**. The complexity of the algorithm largely depends on the *Root* finding strategy for the polynomials. The standard function **Roots** (Input: Polynomial) of MAGMA computer algebra system was used to implement the mentioned algorithm. The complexity of the proposed model would be $O(n^2 \log p)$ for a fixed prime p and supposing that there are n recursive steps that are being performed. *This is a rough estimate and needs further analysis and refinement*.

Remark 2.5.2. In this chapter, we have dealt with odd recursive towers. The *even* case is even more interesting as the properties can be derived in similar ways, but there is a need to prove some basic properties using Cardano's formula and elementary Galois Theory. In the research paper titled *High Order Elements in Finite Fields Arising from Recursive Towers* by Valerio Dose, Pietro Mercuri, Ankan Pal, Claudio Stirpe; we have also dealt with the even recursive towers.

Chapter 3

Class Number Estimation

3.1 Chapter Description

The chapter starts with a description of a key exchange technique used in *Number Field Cryptography* in section 3.2. This section also highlights the efficacy of class number estimation in the field of *Number Field Cryptography*. The main result (Theorem 3.3.2) is about finding a new way to compute the class number for quadratic imaginary number fields $\mathbb{Q}(\sqrt{-p})$ having prime discriminant $p \equiv 3 \bmod 4$; $(p > 3)$.

Remark 3.1.1 (Thematic Scope). The chapter is a result of the studies carried-out by the PhD candidate, with an aim to find *some* applications of the *Finite Transformation Formula* (3.3.1) given by Williams in [Will70]. The *Finite Transformation Formula* is mentioned in our exposition without a proof. There is a vast literature available in the theory of quadratic forms, class numbers, and number field cryptography. Although relevant, but tracing the development of all these theories and aspects would be a massive task, and would steer us away from our specific thematic scope. Hence, only a minuscule amount of background literature is mentioned about number field cryptography in section 3.2 and, class numbers in section 3.3.

3.2 Number Field Cryptography

This section is aimed at illustrating a key exchange in *Number Field Cryptography* (NFC).

Note 3.2.1. This section is mostly collated from the research paper titled *"A Key-Exchange System Based on Imaginary Quadratic Fields" by J Buchmann and HC Williams* [BuWi88]. To read the full reference disclaimer, please refer to [0.1].

Notation: Standard notations and definitions are used from [BuWi88], [Cohn12], [Cox11]. Let, $D < 0$ be a square-free integer, $\mathfrak{K} = \mathbb{Q}[\sqrt{D}]$ be an imaginary quadratic number field, and $\mathcal{Z}$ be the set of rational integers of $\mathfrak{K}$. Let, for any $u, v \in \mathfrak{K}$, $tr(u)$ be the trace of u i.e. sum of u with its conjugate, and $[u, v]$ denote the set $\{u\mathcal{Z} + v\mathcal{Z}\}$. We know that the ring of algebraic integers $\mathcal{O}_{\mathfrak{K}}$ of $\mathfrak{K}$ is given by $[1, \omega]$, where, $\omega = \dfrac{r - 1 + \sqrt{D}}{r}$, and $r = 2$ when $D \equiv 1 \pmod 4$, and $r = 1$ when $D \equiv 2, 3 \ (mod\ 4)$. If, $\mathfrak{a}$ is an ideal of $\mathcal{O}_{\mathfrak{K}}$, then $\mathfrak{a} = [a, b + c\omega]$, where $a, b, c \in \mathcal{Z}$. If there exist non-zero $\alpha, \beta \in \mathcal{O}_{\mathfrak{K}}$ such that $(\alpha)\mathfrak{a} = (\beta)\mathfrak{b}$, we say that $\mathfrak{a}$ and $\mathfrak{b}$ are equivalent ideals of $\mathcal{O}_{\mathfrak{K}}$, and denote this by $\mathfrak{a} \sim \mathfrak{b}$.

An order $\mathcal{O}$ of $\mathfrak{K}$ is a subring $\mathcal{O} \subset \mathcal{O}_{\mathfrak{K}}$, that is also a free $\mathbb{Z}$-module of rank 2 [Klai12]. Consequently, it can be deduced that $\mathcal{O}_{\mathfrak{K}}$ is the maximal order, because it contains every other order. It is well-known that $\mathcal{O}$ and $\mathcal{O}_{\mathfrak{K}}$ are free $\mathbb{Z}$-modules of the same rank [Cox11]. The index $[\mathcal{O}_{\mathfrak{K}} : \mathcal{O}]$ is the conductor of $\mathcal{O}$. This index and the classical definition of conductor (from theory of modules) coincide in the case of quadratic number fields.

Lemma 3.2.1 ([BuWi88])**.** Let the least positive rational integer in any ideal $\mathfrak{c}$ be $L(\mathfrak{c})$. Let $\mathfrak{a}, \mathfrak{b}$ be primitive ideals of $\mathcal{O}_{\mathfrak{K}}$ such that $\mathfrak{a} = [L(\mathfrak{a}), \alpha]$, $\mathfrak{b} = [L(\mathfrak{b}), \beta]$ with $|tr(\alpha)| \leq L(\mathfrak{a})$ and $|tr(\beta)| \leq L(\mathfrak{b})$. If $\mathfrak{a} \sim \mathfrak{b}$, then $L(\mathfrak{a}) = L(\mathfrak{b})$ and $|tr(\alpha)| = |tr(\beta)|$.

Remark 3.2.1 ([Cohn12] [BuWi88]). The ideal $\mathfrak{p}$ is called primitive when it is not divisible by any ideal except the unit ideal (1). An ideal $\mathfrak{q}$ of $\mathcal{O}_{\mathfrak{K}}$ is said to be reduced if $\mathfrak{q}$ is primitive and there does not exist a non-zero $\gamma \in \mathfrak{q}$, such that $|\gamma| < L(\mathfrak{q})$. It can be also shown that each equivalence class of ideals of $\mathcal{O}_{\mathfrak{K}}$ contains a reduced ideal.

Key Exchange [BuWi88]: Alice and Bob select a value of D such that $|D| \geq 10^{200}$ and a ideal $\mathfrak{a}$ in $\mathcal{O}_{\mathfrak{K}}$. The value of D and the ideal $\mathfrak{a}$ is made public.

(1) Alice selects a random integer x and computes a reduced ideal $\mathfrak{b}$ such that $\mathfrak{b} \sim \mathfrak{a}^x$.

(2) Bob selects a random integer y and computes a reduced ideal $\mathfrak{c}$ such that $\mathfrak{c} \sim \mathfrak{a}^y$.

$$A \underset{\mathfrak{c}}{\overset{\mathfrak{b}}{\rightleftarrows}} B$$

Why the Key-Exchange Works? Alice computes a reduced ideal $l_1 \sim \mathfrak{c}^x$ and Bob computes a reduced ideal $l_2 \sim \mathfrak{b}^y$. Since, $l_1 \sim \mathfrak{c}^x \sim (\mathfrak{a}^y)^x = (\mathfrak{a}^x)^y \sim \mathfrak{b}^y \sim l_2$, we can deduce

by lemma 3.2.1 that,

$$L(l_1) = L(l_2).$$

Thus, Alice and Bob can use this (the least positive rational integer $L(l_1)$) as their secret key!

Buchmann and Williams in [BuWi88] remarked that *"No efficient algorithm is known for computing the class number. In fact, computing the class number of an imaginary quadratic order is at least as hard as factoring the discriminant. Hence, imaginary quadratic class groups cannot be used to implement those cryptographic algorithms based on the discrete logarithm problem that require the knowledge of the group order"*. This shows the efficacy of Class Number Estimation in NFC.

This key-exchange illustrates one of the ways in which cryptography can be realized over number fields. Buchmann et. al. in [BuTV04] provides a survey of the infrastructure of quadratic orders that can be used for the development of cryptographic primitives and cryptosystems, which are along the same lines as the aforementioned key exchange. A fast cryptosystem based on non-maximal imaginary quadratic orders was proposed in [HJPT98]. During the end of last century the NICE (New Ideal Coset Encryption) family of cryptosystems were developed in this research area. Jacobson et.al in [JaSW08] also provided the *'real'* counterpart (i.e. NICE Cryptosystems based on Real Quadratic Number Field). One of the noteworthy algebraic aspect of many cryptosystem is that the operations on ciphertexts have coressponding effect on the plaintexts. Although this *homomorphic* property accentuates the usability, but also gives rise to many security flaws in the cryptosystem. In this regard, a *linearly homomorphic encryption scheme* based on composite degree residuosity classes was proposed by Paillier in [Pail99]. Adaptation of this cryptosystem scheme in some quotients of quadratic fields was done by Castagnos in [Cast08]. During his studies, he found that there is an underlying security flaw in NICE cryptosystems, and that the value of the conductor can be easily determined. Hence, Castagnos et. al. in [CaLa09] devised a successful cryptanalysis of the NICE family of cryptosystems on imaginary quadratic fields. They also recommend in [CaLa15] to use the ideas of cryptanalysis of NICE from [CaLa09] for designing a new linearly homomorphic encryption scheme.

An ample amount of literature is available in the field of Number Field Cryptography. But, our aim is not to trace the development of this research area as mentioned in remark 3.1.1. A recent (2019) survey document of Guilhem Castagnos [Cast19] entails a comprehensive account of the relevant literature and tracks the modern development in the field of number field cryptography.

3.3 Evaluation of Class Number

Class Groups have been studied extensively in the nineteenth century, in purview of the theory of quadratic forms. Since then, many elegant theories have been developed in this regard. Dirichlet was deeply fascinated by primes in arithmetic progressions. While studying them, he developed many enigmatic theories alongside enriching the theory of characters and L-functions. He derived a famous formula for class numbers (Th. 3.3.1) which is regarded as one of the cornerstones of analytic theory of numbers. It would be a humongous task to trace the development of the whole theory, and that would steer us away from our thematic scope, as mentioned in remark 3.1.1.

Having said that, we still would like to mention a recent computational achievement in the explicit computation of class groups. In 2019, Beullens et. al. in [BeKV19] reported the computation of the class group of an imaginary quadratic number field having 154-digit discriminant. The interesting aspect is that, they did these computations motivated by a totally different aspect i.e. to develop an efficient isogeny-based digital signature scheme in post quantum cryptography. Although, we do describe an isogeny-based digital signature scheme in chapter 4, but our approach is **not** based on class group computations.

Next, we define *what* is a class number, and then move forward with our exposition on a tiny modification of the class number formula.

Definition 3.3.1 (Ring of Algebraic Integers[IrRo67])**.** A subfield $\mathbb{K}$ of the complex numbers is called an algebraic number field if the index $[\mathbb{K} : \mathbb{Q}]$ is finite. If $\mathbb{K}$ is such a field, the subset of $\mathbb{K}$ consisting of algebraic integers forms a ring $\mathbb{O}$, called the ring of algebraic integers in $\mathbb{K}$.

Definition 3.3.2 (Class Number[IrRo67])**.** Two ideals $A, B \subset \mathbb{O}$ are said to be equivalent, $A \sim B$, if there exists nonzero $\alpha, \beta \in \mathbb{O}$, such that $(\alpha)A = (\beta)B$. *This is an equivalence relation.* The equivalence classes are called ideal classes. The number of ideal classes, h, is called the class number of $\mathbb{K}$.

Remark 3.3.1. Class Number provides us with a measure of the failure of unique factorization in a number field.

Let's recall a famous result of Dirichlet which calculates the class number h_p, of a quadratic imaginary number field of prime discriminant $\mathbb{Q}(\sqrt{-p})$, via a finite sum for $p > 3$. Let, $\left(\frac{\div}{p}\right)$ denote the usual Legendre symbol. For notational convenience we set (as

in [McRa12]),

$$h_p^* := \begin{cases} 0 & p \equiv 1 \mod 4 \\ h_p & p \equiv 3 \mod 4. \end{cases}$$

The following consequence of Dirichlet's class number formula [Dave00, Chapter 6] is well-known,

Theorem 3.3.1 (**Dirichlet** [Dave00]). *For any prime $p > 3$,*

$$h_p^* = -\frac{1}{p}\sum_{x=1}^{p-1} x \left(\frac{x}{p}\right).$$

Williams was interested in computing the sums of Legendre symbols of polynomial functions and in his research paper [Will70] presented the following *Finite Transformation Formula*.

$$\sum_{x=0}^{p-1} \mathcal{F}(x) = \sum_{x=0}^{p-1} \mathcal{F}(x^2) - \sum_{x=0}^{p-1} \left(\frac{x}{p}\right)\mathcal{F}(x), \tag{3.3.1}$$

where, $\left(\frac{\cdot}{p}\right)$ is the usual Legendre Symbol and $\mathcal{F} : \mathbb{Z} \to \mathbb{C}$ is a periodic function with period p. We will use this formula for modifying theorem 3.3.1.

Theorem 3.3.2. *Let $p > 3$ be a prime, and h_p be the class number of a quadratic imaginary number field $\mathbb{Q}[\sqrt{-p}]$. We set,*

$$h_p^* := \begin{cases} 0 & p \equiv 1 \mod 4 \\ h_p & p \equiv 3 \mod 4. \end{cases}$$

Then,

$$h_p^* = \frac{p-1}{2} - \frac{2}{p}\left(\frac{(\lfloor\sqrt{p}\rfloor)(\lfloor\sqrt{p}\rfloor+1)(2\lfloor\sqrt{p}\rfloor+1)}{6} + \sum_{x=\lceil\sqrt{p}\rceil}^{\frac{p-1}{2}} (x^2)_{mod\ p}\right).$$

Proof. We define a *mod p* map $\mathcal{F}' : \mathbb{Z} \to \mathbb{C}$, which is periodic with period p. If we replace $\mathcal{F}$ by $\mathcal{F}'$ in the William's Finite Transformation Formula (equation 3.3.1), we get,

$$-\sum_{x=0}^{p-1} (x)_{mod\ p} \left(\frac{x}{p}\right) = \sum_{x=0}^{p-1} (x)_{mod\ p} - \sum_{x=0}^{p-1} (x^2)_{mod\ p}.$$

An important thing to note is that as we are considering $0 \le x \le p-1$, hence $(x)_{mod\ p} = x$.

But, $(x^2)_{mod\ p} \neq (x\ (mod\ p))^2$. Hence,

$$-\sum_{x=1}^{p-1} x\left(\frac{x}{p}\right) = \sum_{x=1}^{p-1} x - \sum_{x=1}^{p-1} (x^2)_{mod\ p}. \tag{3.3.2}$$

Let, $S = \sum_{x=1}^{p-1} (x^2)_{mod\ p}$. Using Dirichlet's Class Number Formula (theorem 3.3.1) and dividing equation 3.3.2 by p, we get,

$$h_p^* = \frac{p-1}{2} - \frac{S}{p}. \tag{3.3.3}$$

The sum S is a peculiar sum and it can be abbreviated as **SMPS** (**Square** each element then **mod p** then **Sum**). The sum can be further interpreted as the sum of quadratic residues multiplied by a constant (which needs further investigation). As of yet, we can express S in the following way,

$$S = \sum_{x=1}^{p-1} (x^2)_{mod\ p} = 2\left(\sum_{x=1}^{\lfloor\sqrt{p}\rfloor} (x^2)_{mod\ p} + \sum_{x=\lceil\sqrt{p}\rceil}^{\frac{p-1}{2}} (x^2)_{mod\ p}\right).$$

Substituting this in equation 3.3.3, we get,

$$h_p^* = \frac{p-1}{2} - \frac{2}{p}\left(\frac{(\lfloor\sqrt{p}\rfloor)(\lfloor\sqrt{p}\rfloor+1)(2\lfloor\sqrt{p}\rfloor+1)}{6} + \sum_{x=\lceil\sqrt{p}\rceil}^{\frac{p-1}{2}} (x^2)_{mod\ p}\right).$$

□

Remark 3.3.2 (Ongoing Research). This is a part of an ongoing research work of the PhD candidate, and many aspects of the above formula still need to be studied. From the formula, we can immediately deduce that the sum is computed only in the range $\lceil\sqrt{p}\rceil$ *to* $\frac{p-1}{2}$, but for a large p, this would not provide a considerable advantage. Hence, we can *only* suggest that there is a possibility that theorem 3.3.2 might provide an avenue for achieving computational efficiency, subjected to further research.

3.4 Conclusion and Future Work

We encountered a peculiar sum S in the proof of above theorem. By direct computation of this sum, we found the following *computational results*.

- S is divisible by $2p$.
- $h_p^* = S_{\left(mod\ \frac{p+1}{2}\right)} - 1$, where $S_{\left(mod\ \frac{p+1}{2}\right)}$ is the remainder when S is divided by $\frac{p+1}{2}$.
- $S = \sum_{x=1}^{p-1} x = \frac{p(p-1)}{2}$ if $p \equiv 1\ (mod\ 4)$.

We provide a table of Class Numbers and the corresponding sum S in Appendix D.

Note 3.4.1. If we consider the sum S for primes $p \equiv 1\ (mod\ 4)$, then $S = \sum_{x=1}^{p-1} (x^2)_{mod\ p} = \sum_{x=1}^{p-1} x$. The reason for this behavior seems to be that the negative of a residue modulo a prime p is a residue and the negative of a non-residue is a non-residue for primes $p \equiv 1\ (mod\ 4)$, which is a consequence of Gauss' **Quadratic Reciprocity Law**. This might have an effect on the sum $\sum_{x=1}^{p-1} (x^2)_{mod\ p}$. *A further investigation into the distribution of Quadratic Residues is needed to prove this claim.* The future work will follow the techniques given by Aebi and Cairns in [AeCa17].

Chapter 4

Supersingular Isogeny-based Designated Verifier Blind Signature

Note 4.0.1. This chapter is collated from the research paper titled *"Supersingular Isogeny-based Designated Verifier Blind Signature"* by Rajeev Anand Sahu and Agnese Gini and Ankan Pal (PhD candidate), available on IACR, which got five citations in the year 2020. To read the full reference disclaimer, please refer to [0.1].

4.1 Chapter Description

Abstract. An undeniable blind signature scheme constructed by utilizing isogenies of supersingular ellipic curves was proposed by Srinath et al [SrCh16] to provide signer's control in a quantum-resistant blind signature scheme. In this, neither the requester nor the signer can determine a selected verifier apriory. Furthermore, certain weaknesses of undeniable signatures have already been observed and have been overcome by the proposal of designated verifier signature in the classical setting. Following these motivations, we present a quantum-resistant blind signature scheme with a designated verifier, based on isogenies of supersingular elliptic curves. Our construction does not require interactive communication between the signer and the verifier. However, it involves the signer in the verification. This idea of a quantum-resistant blind signature might be useful in specific applications, for example in electronic tendering and online auctioning.

Remark 4.1.1. The proposed signature scheme has shown some vulnerabilities against the attacks designed by Kutas et al in [KMPPS20]. Please refer to remark 4.5.1 in section 4.5 for a preliminary elaboration of this kind of attack.

In this chapter, we discuss a novel idea for a Post-Quantum Isogeny-based Designated Verifier Blind Signature (PQ-DVBS). We start with a broad introduction to the field of Post Quantum Cryptography in subsection 4.2.1. For a basic exposition on isogeny based key exchange, one can refer to subsection 4.2.4. Some of the relevant results about the endomorphisms and isogenies of elliptic curves are discussed in subsection 4.2.2, for providing some theoretical background for the isogeny based key exchange. A broad overview of the literature available on post quantum digital signatures is provided in subsection 4.2.5. In section 4.3, a novel idea for PQ-DVBS is illustrated, named as the two-cube method. In section 4.4, we provide a description of the digital signature scheme, that can be developed using the two-cube method.

4.2 Background

4.2.1 Introduction to Post Quantum Cryptography

A review of the efficacy and urgency of Post-Quantum Cryptography can be found in [BeTa17]. In the recent times, Post-Quantum Cryptography has become one of the key research focus of the cryptographic community. One of the present focal points of the

cryptographic community is to develop relevant literature and develop expertise in this field. One of the key aspects of the Post-Quantum world would be ensuring safe and fast transmission of information in IoT and smart systems. The primary focus is to develop new quantum safe primitives. A two-fold approach which focuses on designing robust cryptographic protocols and assessing the safety through various attack scenarios, is in practice.

The first mathematical model of Quantum Computers was described by RP Feynman [Feyn86] in 1985 along-with other researchers. This heralded the beginning of an active research area in Quantum Information Theory. The key ingredients of this field were Probability Theory and Quantum Mechanics. We have traversed a long and arduous path since then. Quantum Computers are not a far-fetched reality, IBM Inc. [Onl1] has already been able to produce small-scale quantum computing models. Recently, Quantum supremacy was achieved by Google Inc. [AAB919]. Their computational prowess are still in infancy but within few decades, we can expect powerful quantum computers. In the advent of Quantum Computers the Elliptic Curve Discrete Logarithm Problem and RSA would be rendered unsafe, due to Shor's Algorithm [Shor94] (1994). Hence, widely used classical cryptographic protocols would become unsafe, if a sufficiently large quantum computer is engineered. This is the reason for the development of a huge interest of the cryptographic community to come-up with quantum safe protocols.

One of the first quantum key distribution protocol was *BB*84. This protocol used the quantum mechanical phenomenas to safely transmit information. Nonetheless, the stringent limitations on data transmission, and failure under collective sophisticated attack, rendered these protocols inefficient and unsafe [BLMS00]. The cryptographic community again shifted it's focus towards classical Diffie-Hellman Key Exchange (DH-KE), but with a requirement that the safety of such classical protocols should rest on intractable mathematical problems, for which even the quantum algorithms would have an exponential computational time complexity.

This approach worked well and the cryptographic standardization agencies shifted their focus towards this approach. National Institute of Standards and Technologies (NIST) called for submissions of new cryptographic primitives for the standardization of Post Quantum Cryptography. Till February 2021, there have been **three** rounds of submissions comprising of various Public Key Encryptions (PKE), Key Encapsulation Mechanisms (KEM), and Digital Signature Schemes (DSS), for which the details can be found in [Onl2] *(Round **1**)*, [Onl3] *(Round **2**)*, and [Onl4] *(Round **3**)*. The study of post-quantum cryptographic systems is of paramount prominence because of the signs of the advent of extremely dexterous quantum computing devices by the end of the

21^{st} century. This particular paradigm shift in the nature of computing might propel us towards designing better/more secure encryption techniques. We enumerate here the cryptographic paradigms which are viable in the Post-Quantum era.

1. Lattice-based Post-Quantum Cryptography [HoPS98] [Reg09].
2. Code-based Post-Quantum Cryptography [Mcel78].
3. Multivariate Polynomials-based Post-Quantum Cryptography [Pata96].
4. Hash-based Post-Quantum Cryptography [Merk79].
5. Isogeny-based Post-Quantum Cryptography [FeJP14].

We will be discussing some aspects of Isogeny-based Post-Quantum Elliptic Curve Cryptography (IB-PQ-ECC) in this thesis. The computational aspect is intricately related to the theory and structural properties of the elliptic curves. This motivates the exploration of challenging theoretical problems, ranging from Number Theory and Algebra applied to Mathematical Cryptography. In the next subsection, we discuss the Isogenies and Endomorphisms of elliptic curves.

4.2.2 Isogenies and Endomorphisms

Note 4.2.1. This subsection is collated from the books titled *Elliptic Curves: Number Theory and Cryptography by LC Washington* [Wash03] and *The Arithmetic of Elliptic Curves by JH Silverman* [Sil09], and the thesis titled *Post-Quantum Elliptic Curve Cryptography by V Soukharev* [Souk16]. To read the full reference disclaimer, please refer to [0.1].

Remark 4.2.1 (Notation). For this section we set p to be a prime, $q = p^n$, $\mathbb{F}$ to be a field, and $\overline{\mathbb{F}}$ be it's algebraic closure. $\mathbb{F}_q$ be a finite field and $\overline{\mathbb{F}}_q$ as the algebraic closure of $\mathbb{F}_q$. E_i and P_i will be used to denote elliptic curves and the points on it respectively.

We initialize this subsection with the definition of *Torsion Points* (the name is motivated from the theory of Abelian groups).

Definition 4.2.1 (*Torsion Points* [Wash03])**.** Let, E be an elliptic curve defined over a field $\mathbb{F}$ and $\overline{\mathbb{F}}$ is the algebraic closure of $\mathbb{F}$ and $n > 0$. Then the set of *torsion points* is defined as:

$$E[n] = \left\{P \in E(\overline{\mathbb{F}}) \mid nP = O\right\}.$$

Elliptic curves are particularly interesting due to the fact that they can be endowed with a group law (as described in subsection 1.2.1). It is natural then to consider rational

morphisms of curves and view them as group homomorphisms. Isogenies are rational morphisms between elliptic curves, which we define next.

Definition 4.2.2 (*Isogenies* [Sil09])**.** Let, E_1 and E_2 be elliptic curves defined over some field $\mathbb{F}$. An isogeny $\phi : E_1 \to E_2$ is a rational morphism of the form,

$$\phi(x, y) = \left(\frac{f_1(x, y)}{g_1(x, y)}, \frac{f_2(x, y)}{g_2(x, y)}\right),$$

where f_i and g_i are polynomials in x and y.

The point at infinity O satisfies $\phi(O) = O$. We say that any two elliptic curves E_1 and E_2 are isogenous if there is an isogeny either from E_1 to E_2 or E_2 to E_1. We note here that, elliptic curves are algebraic curves, and the degree of an isogeny $\deg \phi$, is its degree as a morphism of algebraic curves. In chapter 1, we dealt with multiplication of points on elliptic curves by an integer. In similar ways, we can define a multiplication map for any integer m, and any point P on the elliptic curve E_1, in the the following way.

$$[m] : E_1 \to E_1, \quad [m](P) = mP.$$

Now, we can state the following theorem, which proves the existence of a corresponding isogeny $\hat{\phi}$ to the isogeny ϕ, and $\hat{\phi}$ will be called as the dual isogeny.

Theorem 4.2.1 (*Dual Isogeny* [Sil09] [Souk16])**.** *Let, E_1, E_2 be elliptic curves over a field $\mathbb{F}$. If, $\phi : E_1 \to E_2$ be an isogeny, then there exists an isogeny $\hat{\phi} : E_2 \to E_1$, such that $\phi \circ \hat{\phi} = [deg\ \phi]$. The isogeny $\hat{\phi}$ is named as the dual isogeny corresponding to the isogeny ϕ.*

It is interesting to note that the degree of the isogeny and its dual are equal. Also, $deg\ \phi$ is an integer, so the map $[deg\ \phi]$ is the multiplication map defined above. Hence, when we compose $\phi \circ \hat{\phi}$, the multiplication map $[deg\ \phi]$ acts on the points of E_2. A conclusion that can be drawn from theorem 4.2.1 is that the function composition $\phi \circ \hat{\phi}$ is commutative.

Definition 4.2.3 (*Separable Isogeny* [Sil09])**.** An Isogeny ϕ can be expressed in terms of polynomials $p(x), q(x), g(x), h(x)$ as,

$$\phi(x, y) = \left(\frac{p(x)}{q(x)}, \frac{g(x)}{h(x)}y\right).$$

We will call an isogeny *separable* when,

$$\frac{d}{dx}\left(\frac{p(x)}{q(x)}\right) \neq 0.$$

In this view, an isogeny (def. 4.2.2) can also be categorized into separable OR (inseparable) if the field extension is separable OR (inseparable). Each separable isogeny can be identified (up to isomorphism) with its kernel ker(ϕ). It can be shown that every isogeny is in fact a group homomorphism [Sil09]. It can be proved that the degree of ϕ is equal to the cardinality of *ker*(ϕ) [Wash03]. An isogeny of degree ℓ is called ℓ-isogeny. In particular, if E_1 is an elliptic curve defined over $\mathbb{F}_q$, and G is a finite subgroup of E_1, then there exists a unique separable isogeny $\phi : E_1 \to E_2$ defined up to $\overline{\mathbb{F}}_q$-isomorphism such that $\ker\phi = G$. We mention some properties of isogenies in the following theorem.

Theorem 4.2.2 ([Sil09]). *Let, E_1, E_2, E_3 be elliptic curves and let $\phi : E_1 \to E_2, \varphi : E_1 \to E_2, \psi : E_2 \to E_3$ be isogenies defined over field $\mathbb{F}$. Then:*

- $\widehat{\psi \circ \phi} = \hat{\phi} \circ \hat{\psi}$.
- $\widehat{\phi + \varphi} = \hat{\phi} + \hat{\varphi}$.
- $\forall m \in \mathbb{Z}, \quad [\hat{m}] = [m] \;\; and \;\; deg[m] = m^2$.
- $deg(\hat{\phi}) = deg(\phi)$.
- $\hat{\hat{\phi}} = \phi$.

If the kernel of an n-isogeny is cyclic then the isogeny is said to be cyclic and we say that the two curves are n-isogenous. Given a prime ℓ, co-prime to the characteristic of the base field, the torsion group $E[\ell]$ is isomorphic to $(\mathbb{Z}/\ell\mathbb{Z})^2$. Hence E has $\ell + 1$ cyclic subgroups of order ℓ and there are (up to isomorphism) exactly $\ell + 1$ distinct (separable) isogenies of degree ℓ with domain E. We continue our foray into understanding the nature of Isogenies and the underlying Endomorphisms of an elliptic curve.

Definition 4.2.4 (*Endomorphism* [Wash03]). α is an Endomorphism of $E(\overline{\mathbb{F}}_q)$ if:

- $\alpha : E(\overline{\mathbb{F}}_q) \to E(\overline{\mathbb{F}}_q)$ is a *Homomorphism*. Therefore, $\alpha(P_1 + P_2) = \alpha(P_1) + \alpha(P_2)$, ($P_1, P_2$ are points on the Elliptic curve E).
- There exists rational functions (quotients of polynomials) $(r_1(x, y), r_2(x, y))$ with coefficients in $\overline{\mathbb{F}}_q$ such that,

$$\alpha(x, y) = (r_1(x, y), r_2(x, y)), \quad \forall\ (x, y) \in E(\overline{\mathbb{F}}_q).$$

Definition 4.2.5 (*Degree of an Endomorphism* [Wash03]). Let, $r_1(x) = \dfrac{h(x)}{g(x)}$ (We Replace y with $\sqrt{x^3 + Ax + B}$). Then, $deg(\alpha) = max(deg(h(x)), deg(g(x)))$. If $\alpha = 0$, then we set $deg(\alpha) = 0$.

Definition 4.2.6 (*Separable Endomorphism* [Wash03])**.** We define $\alpha \neq 0$ to be a separable endomorphism if the derivative $r_1'(x)$ is not identically zero.

We determine elliptic curves as quotients, thus we always identify each curve with its isomorphism class. Moreover, every class of $\overline{\mathbb{F}}_q$-isomorphic curves is uniquely identified by an element of $\overline{\mathbb{F}}_q$, the *j*-invariant. Given an elliptic curve E, its j-invariant $j(E)$ can be computed by the coefficients of a Weierstrass form. Further, whether two elliptic curves are isomorphic or not, can be verified by just comparing their j-invariants.

Definition 4.2.7 (*j-invariant* [Wash03])**.** Let, E be an elliptic curve over a field $\mathbb{F}_q$ such that $char(\mathbb{F}_q) \neq 2$ or 3, then the equation of E is given by $y^2 = x^3 + Ax + B$. We can define the j-invariant of E to be a number $j(E)$ as,

$$j(E) = 1728\frac{4A^3}{4A^3 + 27B^2}.$$

In the next subsection, we will use some of the definitions of this subsection to explain that how supersingular elliptic curves and post quantum cryptography are intricately related to each other.

4.2.3 Supersingular Elliptic Curves and Post Quantum Cryptography

Definition 4.2.8 (*Supersingular Elliptic Curves* [Wash03])**.** Let, E be an elliptic curve over a finite field $\mathbb{F}_p$ of prime characteristic p. If, $E[p]$ be the torsion subgroup [def 4.2.1] such that $E[p]$ is empty, then we label E as a **Supersingular** Elliptic Curve.

In the set of supersingular elliptic curves defined over $\overline{\mathbb{F}}_p$, an isogeny graph is a graph whose nodes represent elliptic curves (up to isomorphism) and edges represent isogenies between them. Let E_1 and E_2 be elliptic curves defined over $\mathbb{F}_p$, then for the isogeny $\phi : E_1 \to E_2$ of degree n, there exists a unique dual isogeny $\hat{\phi} : E_2 \to E_1$, such that $\phi \circ \hat{\phi} = \hat{\phi} \circ \phi = n$, where n is a multiplication map. Hence, isogeny graph can be considered *undirected*.

The set of all endomorphisms of an elliptic curve E, denoted as $End(E)$, forms a ring under the operations of pointwise addition and function composition. If elliptic curve E is defined over a field of positive characteristic, then $End(E)$ is isomorphic either to an order in a quaternion algebra or an order in an imaginary quadratic field. In the first case, the elliptic curve is supersingular and in the latter ordinary. Tate [Tate66] proved that an ordinary and a supersingular curve cannot be isogenous. We would like to highlight the fact that there can never be isogenies between an ordinary elliptic

curve and supersingular elliptic curve. It will be either from ordinary to ordinary or supersingular to supersingular.

In particular, it is possible to prove that the supersingular elliptic curves define a connected component of the isogeny graph whose node can be represented using only $j \in \mathbb{F}_{p^2}$. If we consider only cyclic isogenies of prime degree ℓ, we obtain a $\ell + 1$-regular graph. This ℓ-isogeny graph has many properties, in particular, it has been proved to be an expander graph.

Definition 4.2.9 (*Expander Graphs* [HoLW06])**.** The connected k-regular graphs on n vertices is an expander graph, if there exists an $\epsilon > 0$, such that all non-trivial eigenvalues satisfy $|\lambda| \leq (1 - \epsilon)k$ for large n.

The selection of supersingular curves is substantiated by the fact that it has a larger endomorphism ring than the ordinary curves. Also, if we use the non-supersingular elliptic curves, then it can be shown that the security of the Isogeny-based DH-KE reduces to a 'Abelian Hidden Shift/Subgroup Problem' [4.2.10] in a group [Souk16] for which sub-exponential quantum algorithms exist.

Definition 4.2.10 (*Abelian Hidden Shift Problem* [Souk16])**.** Let, A be a known finite abelian group and let the maps f_0, f_1 hide a shift $s \in A$ if f_0 is injective and $f_1(x) = f_0(xs)$ (ie, f_1 is a shifted version of f_0). The goal of the hidden shift problem is to determine s, using queries to such blackbox functions.

Supersingular isogenies were first introduced in cryptography by Charles, Goren and Lauter [ChLG09]. The pivotal idea that they used was of the Deuring correspondence. This is a one-to-one correspondence between the j-invariants of the supersingular elliptic curves and the maximal orders in a quarternion algebra, up to some equivalence relation. The strategy is implemented in a threefold way - the correspondence allows to transform an isogeny problem into its quartenion algebra equivalent problem, solving it there, and then again translating it back to the solution of the isogeny problem. The hardness of this strategy depends on finding paths in supersingular isogeny graphs [PeLa17]. These isogeny graphs are expander graphs and have the Ramanujan property, for which there is presently, no sub-exponential time algorithm to find the specific paths of the graphs, even in the quantum computing paradigm. Hence, supersingular elliptic curves are suitable candidates for Post-Quantum Isogeny-based Cryptography. In the next subsection we will be elucidating the idea of a key exchange using isogenies of supersingular elliptic curves.

4.2.4 Isogeny-based Key Exchange

In a strictly categorical sense, we intend to study the rational morphisms along with the mathematical structure of elliptic curves. Typically, the Elliptic Curve Discrete

Logarithm Problem (EC-DLP) relies on the structural properties of the abelian variety. The morphisms do not play a pivotal role in EC-DLP. Usually, the classical cryptosystems rely on structures rather than the morphisms. In the post-quantum era there would be a paradigm shift and the study of the morphisms would play an important role in cryptography. The rational maps (isogenies) of the supersingular elliptic curves are a direct component of the design and construction of the post quantum elliptic curve cryptography. To recapitulate, the underlying hard problem for isogeny-based cryptography is - *Given two isogenous supersingular elliptic curves,* ***Find*** *an isogeny between them*. Currently no quantum algorithm is known for solving this problem in general in polynomial time.

In the Encryption-Decryption stage of Isogeny-based Post Quantum Elliptic Curve Cryptography, the isogenies can be computed using Velu's formula [Velu71]. Nonetheless, it is a quantum resistant cryptosystem because the security depends on deciphering information about the endomorphism ring $End(E(\mathbb{F}_p))$ of a supersingular elliptic curve over a finite field $E(\mathbb{F}_p)$; and presently there is no algorithm which can solve this problem in polynomial time. Now, we provide an illustration of a *Isogeny-based Key Exchange* described in [FeJP14]. The following version is quoted from [Souk16].

- We fix as public parameters a supersingular elliptic curve E_0 defined over $\mathbb{F}_{p^2}$, and bases $\{P_A, Q_A\}$ and $\{P_B, Q_B\}$ which generate $E_0[{l_A}^{e_A}]$ and $E_0[{l_B}^{e_B}]$ respectively, so that, $< P_A, Q_A >= E_0[{l_A}^{e_A}]$ and $< P_B, Q_B >= E_0[{l_B}^{e_B}]$. All torsion groups are always defined over $\mathbb{F}_{p^2}$, hence this requires picking a curve having the correct order over $\mathbb{F}_{p^2}$.
- Alice chooses two random elements $m_A, n_A \in \mathbb{Z}/{l_A}^{e_A}\mathbb{Z}$, not both divisible by l_A.
- Alice computes an isogeny $\phi_A : E_0 \to E_A$ with kernel $K_A := < [m_A]P_A + [n_A]Q_A >$.
- Alice computes the image $\{\phi_A(P_B), \phi_A(Q_B)\} \subset E_A$ of the basis $\{P_B, Q_B\}$ for $E_0[{l_B}^{e_B}]$ under her secret isogeny ϕ_A, and sends these points to Bob together with E_A. Similarly, Bob selects random elements $m_B, n_B \in \mathbb{Z}/{l_B}^{e_B}\mathbb{Z}$.
- Bob computes an isogeny $\phi_B : E_0 \to E_B$ having kernel $K_B :=< [m_B]P_B + [n_B]Q_B >$, along with the points $\{\phi_B(P_A), \phi_B(Q_A)\}$.
- Bob sends E_B *and* $\{\phi_B(P_A), \phi_B(Q_A)\} \in E_B$.
- Alice computes an isogeny $\phi_A{}' : E_B \to E_{AB}$ having kernel equal to $< [m_A]\phi_B(P_A) + [n_A]\phi_B(Q_A) >$.

Alice and Bob can then use the common j-invariant of,

$$E_{AB} = \phi_B{}'(\phi_A(E_0)) = \phi_A{}'(\phi_B(E_0)) = E_0/ < [m_A]P_A + [n_A]Q_A, [m_B]P_B + [n_B]Q_B >,$$

to form a shared secret key!

After understanding the key-exchange, it is a good point where we can take a step further, and divulge into the designing of a Digital Signature Scheme. Usually, in the field of cryptography, designing a sound and secure *Digital Signatures* is supposed to be a challenging problem. In the next subsection, we provide a short introduction to the relevant literature about digital signatures in the post-quantum era.

4.2.5 Post Quantum Digital Signatures

This subsection provides an introductory literature survey about Digital Signatures in the post-quantum setting. In his doctoral thesis, Stolbunov [Stol12] outlined a probable idea of digital signature scheme (DSS) from isogenies, but strong designated verifier signature by Xi et al [SuTW12] and undeniable signature of Jao and Soukharev [JaSo14] were the initial concrete signature schemes, using the properties of isogenies [4.2.2] between supersingular elliptic curves [4.2.8]. A generalization of the isogeny-based DSS, from supersingular elliptic curves, were presented by Galbraith et al [GaPS17] and Yoo et. al. [YAJJS17]. The first signature of [GaPS17] and the signature of [YAJJS17] were obtained by Unruh's transformation [Unruh15] (which can be viewed as a quantum analogue of the Fiat-Shamir transform [FiSh86]), on the De Feo-Jao-Plut [FeJP14]. The signature in [GaPS17] achieves space optimization due to smaller size than that of [YAJJS17].

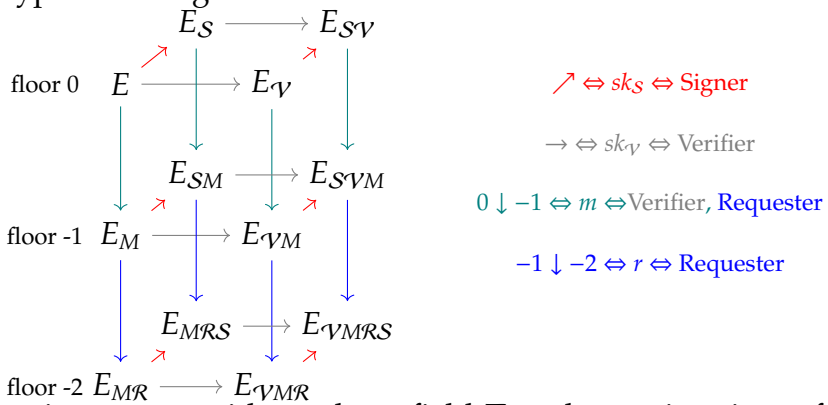
To achieve off-line anonymity, David Chaum [Chaum83] introduced the idea of blind signatures. It is a two-party interactive protocol, where a requester receives the signature(s) with the message(s) from a signer such that the actual message and signature, (both) are blinded. Due to its property of anonymity, this signature finds excellent applications in electronic cash system, viz. untraceable payments, and electronic voting system etc. The main security requirements of blind signature are unforgeability and blindness. Security challenges of blind signature are studied in detail and addressed in [PoSt00] [ScUn17]. The idea of undeniable signature [ChVa89] was introduced to provide signer's control in the signature verification. This was obtained by directly involving the signer in the verification procedure. The signer can decide when a signature has to be verified, but not *who (or how many)* can be verified. Such a signature is useful in various applications like licensing software etc.

Unfortunately, certain fundamental weaknesses [DeYu91], blackmailing [Jakob94], and man-in-the-middle attack [DeGB87] have been observed for the undeniable signature which affects the practical applications. An obvious roadblock is the requirement that the signer be available online (always) for the verification. To address the observed weaknesses of the undeniable signature, designated verifier signature (DVS) [JaSI96] was proposed. A DVS is issued for an authorized verifier who can only verify the signature but cannot transfer the conviction of verification to any third party.

In this section, we have tried to provide a bird's overview of the background and some relevant literature, which is needed to understand the implementation of the Two-cube method.

4.3 Two Cube Method

The two-cube method is a small step towards generalizing the concept of isogeny based signatures for multi-party communication. In this method, we will see that, how the Requester $\mathcal{R}$, the Signer $\mathcal{S}$, and the Verifier $\mathcal{V}$, communicate between each other, and send the the encrypted message $\mathcal{M}$. The degree of the isogenies that are used in the two-cube method are prime powers. The isogenies are separable and cyclic. Under these assumptions, we do not need to identify the isogenies with a n-cyclic torsion subgroup of the elliptic curve. The isogenies and the image points are always defined upto isomorphism. Hence, we deal with class of isomorphic curves whose j-invariant is same. The curves would always imply a class of isomorphic curves whose j-invariant are the same and vice versa (the j-invariant would be the representative of the class). We provide a brief account of the two-cube method with the help of following diagrams. In the diagrams, the subscript $\mathcal{R}$ is used for Requester, $\mathcal{S}$ for Signer, $\mathcal{V}$ for Verifier, and $\mathcal{M}$ for the encrypted message.



In our construction, we consider as base field $\mathbb{F}_{p^2}$ where p is prime of the form $p = \ell_{\mathcal{R}}\ell_{\mathcal{S}}^{e_{\mathcal{S}}}\ell_{\mathcal{V}}^{e_{\mathcal{V}}}\ell_{M}^{e_{M}} f \pm 1$, where ℓ_i are distinct small primes, e_i are positive integers and $f \geq 1$ is a small cofactor. We fix a supersingular curve E over $\mathbb{F}_{p^2}$ and $\{P_{\mathcal{R}}, Q_{\mathcal{R}}\}, \{P_{\mathcal{S}}, Q_{\mathcal{S}}\}$,

$\{P_{\mathcal{V}}, Q_{\mathcal{V}}\}$, and $\{P_M, Q_M\}$ bases of the $\ell_{\mathcal{R}}^{e_{\mathcal{R}}}$, $\ell_{\mathcal{S}}^{e_{\mathcal{S}}}$, $\ell_{\mathcal{V}}^{e_{\mathcal{V}}}$, and $\ell_M^{e_M}$-torsion groups respectively. In the following diagrams, we describe the isogenies involved.

$$\begin{array}{ccc} E & \xrightarrow{\phi_{\mathcal{S}}} & E_{\mathcal{S}} \\ {\scriptstyle \phi_{\mathcal{V}}}\downarrow & & \downarrow{\scriptstyle \phi_{\mathcal{S}\mathcal{V}}} \\ E_{\mathcal{V}} & \xrightarrow{\phi_{\mathcal{V}\mathcal{S}}} & E_{\mathcal{S}\mathcal{V}} \end{array} \qquad \begin{array}{ccc} E_{\mathcal{V}} & \xrightarrow{\phi_{\mathcal{V}\mathcal{S}}} & E_{\mathcal{V}\mathcal{S}} \\ {\scriptstyle \phi_{\mathcal{V}M}}\downarrow & & \downarrow{\scriptstyle \phi_{\mathcal{V}\mathcal{S}M}} \\ E_{\mathcal{V}M} & \xrightarrow{\phi_{\mathcal{V}M\mathcal{S}}} & E_{\mathcal{V}\mathcal{S}M} \end{array}$$

We use this method to propose the *Supersingular Isogeny-based Digital Signature Scheme* with a *Designated Verifier*.

4.4 Proposed Digital Signature Scheme

There are three users in the scheme, the requester $\mathcal{R}$ who requests signature on a blinded message from the signer, the signer $\mathcal{S}$ who signs the blinded messages for the requester and the verifier $\mathcal{V}$ who verifies the signature received from the requester. The structure of scheme is as follows.

1. $params \leftarrow \mathsf{Setup}(\lambda)$: This Setup algorithm, on input of security parameter λ, generates the system's public parameters *params*. In all the algorithms, *params* will be considered as an implicit input.
2. $(pk, sk) \leftarrow \mathsf{KeyGen}(params)$: This key generation algorithm, on input of *params*, generates user's (public key, private/secret key) pair (pk, sk). It also outputs system's fixed public value E, P_{pub}.
3. $\sigma \leftarrow \mathsf{Sign}(\mathsf{sk}_{\mathcal{S}}, \mathsf{pk}_{\mathcal{V}}, \mathsf{m})$: This is the signature algorithm. On input of the signing key $sk_{\mathcal{S}}$ of signer, public key $pk_{\mathcal{V}}$ of verifier and the message m, this probabilistic (or deterministic) algorithm finally generates σ. This main algorithm consists of the following three sub-routines,
   (a) $m' \leftarrow \mathsf{Blinding}(\mathsf{m}, \mathsf{r})$: This is a probabilistic blinding algorithm which takes the input message m, a random input r and outputs the blinded message m'.
   (b) $\sigma' \leftarrow \mathsf{Sign}(\mathsf{m}', \mathsf{sk}_{\mathcal{S}}, \mathsf{pk}_{\mathcal{V}})$: This is a signing algorithm run by the signer by taking inputs of the blinded message m', secret key $sk_{\mathcal{S}}$ of the signer, and public key $pk_{\mathcal{V}}$ of the verifier. This algorithm outputs signature σ' on message m'.
   (c) $\sigma \leftarrow \mathsf{Unblinding}(\sigma')$: This is a deterministic unblinding algorithm, which outputs the unblinded signature σ on message m, after taking the blinded signature σ' as an input.

4. $b \leftarrow \mathsf{Verify}(\mathsf{sk}_{\mathcal{V}}, \mathsf{pk}_{\mathcal{S}}, \sigma, \mathsf{m})$: This is the deterministic verification algorithm run by the designated verifier. On input of the secret key $sk_{\mathcal{V}}$ of the verifier, public key $pk_{\mathcal{S}}$ of signer, signature σ, and the message m, this deterministic algorithm outputs a bit b which is 1 if the signature is valid and 0 if invalid.

The proposed scheme consists the algorithms - Setup, KeyGen, Sign and Verify.

Setup: This algorithm generates the system's public parameters

$$params = (p, E, \{P_{\mathcal{R}}, Q_{\mathcal{R}}\}, \{P_{\mathcal{S}}, Q_{\mathcal{S}}\}, \{P_{\mathcal{V}}, Q_{\mathcal{V}}\}, \{P_M, Q_M\}, H),$$

where p is a prime of the form $\ell_{\mathcal{R}}^{e_{\mathcal{R}}}\ell_{\mathcal{S}}^{e_{\mathcal{S}}}\ell_{\mathcal{V}}^{e_{\mathcal{V}}}\ell_M^{e_M} \cdot f \pm 1$, E is a supersingular elliptic curve over $\mathbb{F}_{p^2}$ such that $\#E(\mathbb{F}_{p^2})$ is divisible by $(\ell_{\mathcal{R}}^{e_{\mathcal{R}}}\ell_{\mathcal{S}}^{e_{\mathcal{S}}}\ell_{\mathcal{V}}^{e_{\mathcal{V}}}\ell_M^{e_M})^2$, $\{P_{\mathcal{R}}, Q_{\mathcal{R}}\}, \{P_{\mathcal{S}}, Q_{\mathcal{S}}\}, \{P_{\mathcal{V}}, Q_{\mathcal{V}}\}, \{P_M, Q_M\}$ are points which generates $E[\ell_{\mathcal{R}}^{e_{\mathcal{R}}}], E[\ell_{\mathcal{S}}^{e_{\mathcal{S}}}], E[\ell_{\mathcal{V}}^{e_{\mathcal{V}}}], E[\ell_M^{e_M}]$ respectively, and $H : \{0,1\}^* \rightarrow \frac{\mathbb{Z}}{\ell_M^{e_M}\mathbb{Z}}$ is a cryptographic hash function.

KeyGen: The signer and verifier generates their respective public key and private key as follows:

Singer's Public Key: $E_{\mathcal{S}}, \phi_{\mathcal{S}}(P_{\mathcal{V}}), \phi_{\mathcal{S}}(Q_{\mathcal{V}}), \phi_{\mathcal{S}}(P_M), \phi_{\mathcal{S}}(Q_M)$.

Signer's Private Key: $m_{\mathcal{S}}, n_{\mathcal{S}}, K_{\mathcal{S}}, \phi_{\mathcal{S}}$.

Verifier's Public Key: $E_{\mathcal{V}}, \phi_{\mathcal{V}}(P_M), \phi_{\mathcal{V}}(Q_M), \phi_{\mathcal{V}}(P_{\mathcal{S}}), \phi_{\mathcal{V}}(Q_{\mathcal{S}}), \phi_{\mathcal{V}}(P_{\mathcal{R}}), \phi_{\mathcal{V}}(Q_{\mathcal{R}})$.

Verifier's Private Key: $m_{\mathcal{V}}, n_{\mathcal{V}} \in \frac{\mathbb{Z}}{\ell_M^{e_M}\mathbb{Z}}, K_{\mathcal{V}}, \phi_{\mathcal{V}}$.

Here, $m_{\mathcal{S}}, n_{\mathcal{S}}, m_{\mathcal{V}}, n_{\mathcal{V}} \in \frac{\mathbb{Z}}{\ell_M^{e_M}\mathbb{Z}}$ and $K_{\mathcal{S}} = [m_{\mathcal{S}}]P_{\mathcal{S}} + [n_{\mathcal{S}}]Q_{\mathcal{S}}$, $K_{\mathcal{V}} = [m_{\mathcal{V}}]P_{\mathcal{V}} + [n_{\mathcal{V}}]Q_{\mathcal{V}}$.

Sign: This has 3 sub-algorithms:

Blinding: The blinding requires two steps which are enumerated below.

Hashing: Let M be the message to be signed. The requester computes the hash $h = H(M)$, and the isogenies ϕ_M and $\phi_{\mathcal{V}M}$ whose codomains are respectively the curves,

$$E_M = \frac{E}{\langle P_M + hQ_M \rangle} \ ,$$

and

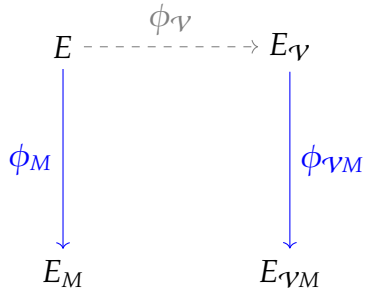
$$E_{\mathcal{V}M} = \frac{E_{\mathcal{V}}}{\langle \phi_{\mathcal{V}}(P_M) + h\phi_{\mathcal{V}}(Q_M) \rangle} \ .$$

Additionally, the following images are computed,

$$\phi_M(P_{\mathcal{R}}), \phi_M(Q_{\mathcal{R}}), \phi_M(P_{\mathcal{V}}), \phi_M(Q_{\mathcal{V}}), \phi_M(P_{\mathcal{S}}), \phi_M(Q_{\mathcal{S}}),$$

and

$$\phi_{\mathcal{V}M}(\phi_{\mathcal{V}}(P_{\mathcal{R}})), \phi_{\mathcal{V}M}(\phi_{\mathcal{V}}(Q_{\mathcal{R}})), \phi_{\mathcal{V}M}(\phi_{\mathcal{V}}(P_{\mathcal{S}})), \phi_{\mathcal{V}M}(\phi_{\mathcal{V}}(Q_{\mathcal{S}})).$$

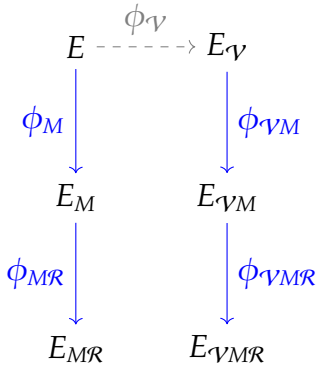


Blinding: The requester selects $r \in \mathbb{Z}/\ell_{\mathcal{R}}^{e_{\mathcal{R}}}\mathbb{Z}$ randomly and computes the isogenies $\phi_{M\mathcal{R}}$ and $\phi_{\mathcal{V}M\mathcal{R}}$ whose codomains are respectively,

$$E_{M\mathcal{R}} = \frac{E_M}{\langle \phi_M(P_{\mathcal{R}}) + r \cdot \phi_M(Q_{\mathcal{R}}) \rangle} ,$$

and

$$E_{\mathcal{V}M\mathcal{R}} = \frac{E_{\mathcal{V}M}}{\langle \phi_{\mathcal{V}M}(\phi_{\mathcal{V}}(P_{\mathcal{R}})) + r \cdot \phi_{\mathcal{V}M}(\phi_{\mathcal{V}}(Q_{\mathcal{R}})) \rangle} .$$



The signing protocol is inspired by the one in [SrCh16]. In particular, we need to compute the "dual" isogenies of $\phi_{M\mathcal{R}}$ and $\phi_{\mathcal{V}M\mathcal{R}}$ to make the unblinding possible. We refer to [SrCh16, Section 4, Remark 4.1)], for details. Here, we recall the main operations in order to establish a coherent notation in our setting.

The requester has to find two points $K \in E_M[\ell_{\mathcal{R}}^{e_{\mathcal{R}}}]$ and $K_{\mathcal{V}} \in E_{\mathcal{V}M}[\ell_{\mathcal{R}}^{e_{\mathcal{R}}}]$ of order exactly $\ell_{\mathcal{R}}^{e_{\mathcal{R}}}$ such that $K \notin \ker \phi_{M\mathcal{R}}$ and $K_{\mathcal{V}} \notin \ker \phi_{\mathcal{V}M\mathcal{R}}$. Now, two random bases $\left\{P'_{\mathcal{R}}, Q'_{\mathcal{R}}\right\}$ of $E_{M\mathcal{R}}[\ell_{\mathcal{R}}^{e_{\mathcal{R}}}]$ and $\left\{P''_{\mathcal{R}}, Q''_{\mathcal{R}}\right\}$ of $E_{\mathcal{V}M\mathcal{R}}[\ell_{\mathcal{R}}^{e_{\mathcal{R}}}]$ are chosen,

$m', n', m'', n'' \in \mathbb{Z}/\ell_{\mathcal{R}}^{e_{\mathcal{R}}}\mathbb{Z}$ are computed such that,

$$\phi_{M\mathcal{R}}(K) = m'\phi_{M\mathcal{R}}(P'_{\mathcal{R}}) + n'\phi_{M\mathcal{R}}(Q'_{\mathcal{R}}),$$

and

$$\phi_{\mathcal{V}M\mathcal{R}}(K_{\mathcal{V}}) = m''\phi_{\mathcal{V}M\mathcal{R}}(P''_{\mathcal{R}}) + n''\phi_{\mathcal{V}M\mathcal{R}}(Q''_{\mathcal{R}}).$$

Now, $E_{M\mathcal{R}}, E_{\mathcal{V}M\mathcal{R}}, \left\{P'_{\mathcal{R}}, Q'_{\mathcal{R}}\right\}$ *and* $\left\{P''_{\mathcal{R}}, Q''_{\mathcal{R}}\right\}$, and the following images are sent to the signer,

$$\phi_{M\mathcal{R}}(\phi_M(P_{\mathcal{V}})), \phi_{M\mathcal{R}}(\phi_M(Q_{\mathcal{V}})), \phi_{M\mathcal{R}}(\phi_M(P_{\mathcal{S}})), \phi_{M\mathcal{R}}(\phi_M(Q_{\mathcal{S}})),$$

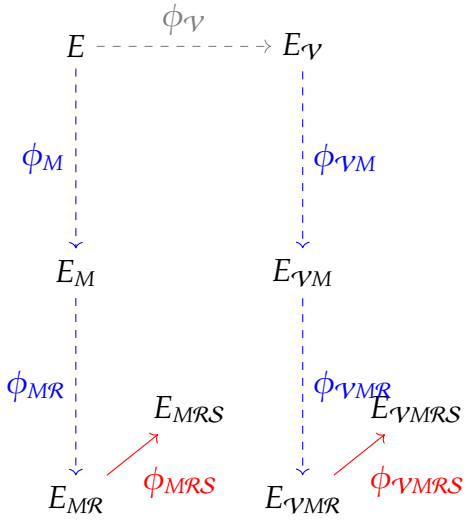
and

$$\phi_{\mathcal{V}M\mathcal{R}}(\phi_{\mathcal{V}M}(\phi_{\mathcal{V}}(P_{\mathcal{S}}))), \phi_{\mathcal{V}M\mathcal{R}}(\phi_{\mathcal{V}M}(\phi_{\mathcal{V}}(Q_{\mathcal{S}}))).$$

Sign: The signer computes the curves,

$$E_{M\mathcal{R}\mathcal{S}} = \frac{E_{M\mathcal{R}}}{\langle m_{\mathcal{S}}\phi_{M\mathcal{R}}(\phi_M(P_{\mathcal{S}})) + n_{\mathcal{S}}\phi_{M\mathcal{R}}(\phi_M(Q_{\mathcal{S}}))\rangle},$$

$$E_{\mathcal{V}M\mathcal{R}\mathcal{S}} = \frac{E_{\mathcal{V}M\mathcal{R}}}{\langle m_{\mathcal{S}}\phi_{\mathcal{V}M\mathcal{R}}(\phi_{\mathcal{V}M}(\phi_{\mathcal{V}}(P_{\mathcal{S}}))) + n_{\mathcal{S}}\phi_{\mathcal{V}M\mathcal{R}}(\phi_{\mathcal{V}M}(\phi_{\mathcal{V}}(Q_{\mathcal{S}})))\rangle}.$$



The signer provides $E_{M\mathcal{R}\mathcal{S}}, E_{\mathcal{V}M\mathcal{R}\mathcal{S}}$ and

$$\phi_{M\mathcal{R}\mathcal{S}}(\phi_{M\mathcal{R}}(\phi_M(P_{\mathcal{V}}))), \phi_{M\mathcal{R}\mathcal{S}}(\phi_{M\mathcal{R}}(\phi_M(Q_{\mathcal{V}}))),$$

$$\phi_{M\mathcal{R}\mathcal{S}}(P'_{\mathcal{R}}), \phi_{M\mathcal{R}\mathcal{S}}(Q'_{\mathcal{R}}), \phi_{\mathcal{V}M\mathcal{R}\mathcal{S}}(P''_{\mathcal{R}}), \phi_{\mathcal{V}M\mathcal{R}\mathcal{S}}(Q''_{\mathcal{R}}),$$

to the requester as the signature on the blinded message $(E_{M\mathcal{R}}, E_{\mathcal{V}M\mathcal{R}})$.

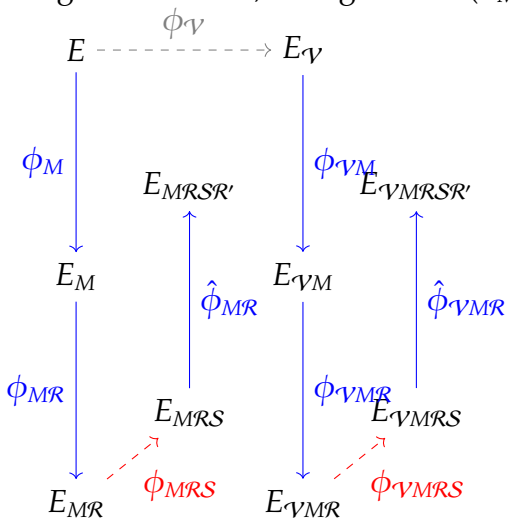
Unblinding: Receiving the signature on the blinded message, the requester generates the signature on the original message as,

$$E_{\mathcal{MRSR}'} = \frac{E_{\mathcal{MRS}}}{\langle m \cdot \phi_{\mathcal{MRS}}(P_{\mathcal{R}'}) + n \cdot \phi_{\mathcal{MRS}}(Q_{\mathcal{R}'})\rangle} \ ,$$

and

$$E_{\mathcal{VMRSR}''} = \frac{E_{\mathcal{VMRS}}}{\langle m' \cdot \phi_{\mathcal{VMRS}}(P_{\mathcal{R}''}) + n' \cdot \phi_{\mathcal{VMRS}}(Q_{\mathcal{R}''})\rangle} \ ,$$

then computes $\tilde{P}_{\mathcal{V}} = \hat{\phi}_{\mathcal{MR}}(\phi_{\mathcal{MRS}}(P'_{\mathcal{R}}))$ and $\tilde{Q}_{\mathcal{V}} = \hat{\phi}_{\mathcal{MR}}(\phi_{\mathcal{MRS}}(Q'_{\mathcal{R}}))$. Finally, the requester provides the designated verifier, the signature $\sigma(E_{\mathcal{MRSR}'}, E_{\mathcal{VMRSR}''}, \tilde{P}_{\mathcal{V}}, \tilde{Q}_{\mathcal{V}})$



Verify To verify the received signature, the designated verifier proceeds as follows. The process is initialized in the following way.

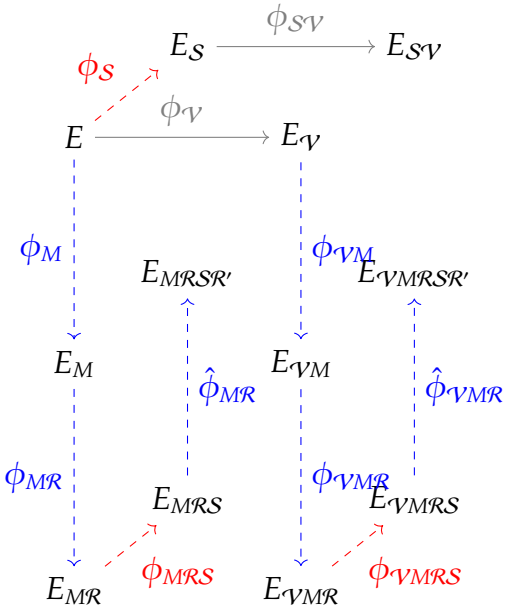
$$E_{\mathcal{SV}} = \frac{E_{\mathcal{S}}}{\langle m_{\mathcal{V}} \cdot \phi_{\mathcal{S}}(P_{\mathcal{V}}) + n_{\mathcal{V}} \cdot \phi_{\mathcal{S}}(Q_{\mathcal{V}})\rangle} \ ,$$

and

$$E_{\mathcal{SVM}} = \frac{E_{\mathcal{SV}}}{\langle \phi_{\mathcal{SV}}(\phi_{\mathcal{S}}(P_M)) + h \cdot \phi_{\mathcal{SV}}(\phi_{\mathcal{S}}(Q_M))\rangle} \ ,$$

and

$$E_{\mathcal{SM}} = \frac{E_{\mathcal{S}}}{\langle \phi_{\mathcal{S}}(P_M) + h \cdot \phi_{\mathcal{S}}(Q_M)\rangle} \ .$$



The verifier accepts the signature if $j(E_{\mathcal{V}M\mathcal{R}S\mathcal{R}''}) = j(E_{\mathcal{SV}M})$ and $j(E_{M\mathcal{R}S\mathcal{R}'}) = j(E_{\mathcal{S}M})$.

4.5 Conclusion and Future Work

In the preceding section, we can verify the proof of concept for developing a digital signature using the two-cube method. The security of the proposed signature scheme relies on the difficulty of computing an isogeny between two given supersingular elliptic curves. As in other schemes, the degree of the isogenies involved in our scheme are public. In order to compute an isogeny between two given curves, one of the solution is to explore the isogeny graph using a meet-in-the-middle strategy. But, these kind of attacks are more effective if some vulnerabilities are detected in the digital signature scheme or key-exchange protocol. In this regard, the main vulnerabilities of SIDH-variants (the 2-cube method belongs to the same family), that are exploited in [KMPPS20] are based on the torsion-point attack designed by [Petit17].

Remark 4.5.1 (Vulnerabilities). In [Petit17], Petit shows that the information about images of torsion-points can lead to the design of successful attacks on the Isogeny-based key exchange. In [KMPPS20], Kutas et. al. generalize it for broader choice of initial parameters for many SIDH variants. They also show that, weak choice of E_0 (base curve) under imbalanced parameters as well as weak choice of base field under balanced parameters, can lead to successful attacks. During unblinding of the signature in the proposed scheme (Section 4.4), there is a partial and insecure transmission of the torsion-point images, for which the attack as described in [KMPPS20] might be effective. Although, this can be ameliorated by the use of effective unblinding procedure, which is

still a problem to *ponder about*. This is also a roadblock towards achieving robustness of the proposed signature scheme. Also, the imbalanced parameter choices initially makes the proposed signature scheme susceptible to the attacks of [KMPPS20]. But, this can be easily mitigated through better choice of initial parameters or changing the base curve E_0.

Remark 4.5.2 (Complexity). As discussed throughout the chapter that the main advantage of isogeny based cryptography is that, computing isogenies is fast. This is the key component in the encryption procedure. Velu's formula [Velu71] provides an explicit method to compute isogenies with a quadratic complexity. Also, a great improvement is due to the Schoof-Elkies-Atkins algorithm [Scho95] for point counting, which has a complexity of $O(n^{4+\epsilon})$, where n is the number of bits required to express the total number of elements in the finite field or its extension. The complexity of the proposed signature is similar to that of [FeJP14], which is *roughly* estimated to be $O(\ell^3 + n^{4+\epsilon})$, where ℓ is the degree of the isogeny that we want to compute.

Note 4.5.1. In this thesis, we have elucidated only the novel two-cube method, to illustrate that how isogenies of the supersingular elliptic curves can be utilized for Cryptography. In the research paper titled *Supersingular Isogeny-Based Designated Verifier Blind Signature* by Rajeev Anand Sahu, Agnese Gini, and Ankan Pal; we have discussed the security proofs. But, the mentioned Digital Signature is not *yet* strong enough to ward off the threats posed by the attacks designed by Kutas et al in [KMPPS20].

Appendix A. Algorithm for Intersection Method

The algorithm consists of steps which depends on accessing the points on the elliptic curve and operating on them to implement the idea of intersection of curves. It starts with initialization of the finite field and constructing an elliptic curve over it. Then we generate a polynomial ring and define the required polynomials. The vanishing ideals are evaluated henceforth, and the derivative is computed. After this, Grobner basis is computed and the $F4$ algorithm is implemented to solve the system of equations. The algorithm is realized through MAGMA [BoCa93]. We hereby provide the pseudocode for the the sub-routines of the algorithm. The code is available here.

Algorithm 1: Intersection Method

Construct $F := FiniteField(p, k)$, $E := EllipticCurve([F|A, B])$, and $P \in E$;
/* $p \geq 5$ is a prime number, A and B are the coefficients in the equation of elliptic curve. */
for $s = 0;\ s < m_1;\ s = s + 1$ **do**
  define ps as $[2^s * P]$
end
/* Operation on the point P. $m := Floor(Log(2, n))$. $m_1 = m - 1, m_2 = m - 2$ and similarly we can continue. */
Construct $R := PolynomialRing(F, 2m)$ and $PolynomialRing(R, 2)$;
/* The variables are w and k respetively. */
for $i = 1;\ i < m;\ i = i + 1$ **do**
  define h as $w[i]$
end
/* Array of coefficients. */
Construct $H := Polynomial(h)$ and $G := Polynomial(g)$;
/* Variables are u and v respectively. */
$Evaluate(H, k[1])$ and $Evaluate(G, k[1]) + k[1]^{m_2}$;
/* Evaluating the Polynomial. */
for $i = 1;\ i < (\#T + 1);\ i = i + 1$ **do**
  define Z as $[Evaluate(f, T[i])]$
end
/* From array ps, an array of arrays T is constructed. f is defined as the sum of the evaluations from the previous steps, and expressed in variables x_1 and y_1. */
Construct an ideal i_1 as $< R|Z >$;
/* Initializing the ideal for calculating the vanishing ideal. i_2, i_3, i_4, i_5 ideals are constructed consequently. */
$Evaluate(Derivative(r, k[1]))$;
/* $r = x_1^2 - k[1]^3 * y_1^2 - A * k[1] * y_1^2 - B * y_1^2$. */
Initialize Q as $(n - 100) * P$;
Compute $Radical(i_5)$, $Groebner(R)$, $PrimaryDecomposition(R)$, $GroebnerBasis(R[1])$;
for $i = 1;\ i < (\#Z + 1);\ i = i + 1$ **do**
  if $Z[i] = 0$ **then**
    Set $Z_1 = [0]$
  end
  else
    set $Z_1 = [Z[i]]$
  end
end
/* Z is constructed as the array of arrays of the primary decomposition. */
for $i = 1;\ i < (\#Z + 1);\ i = i + 1$ **do**
  if $Z_1[i] = 0$ **then**
    set $Z_2 = [0]$
  end
  else
    set $Z_2 = [2^{(Z_1[i])}]$
  end
end

Appendix B. Algorithm for Odd Recursive Towers

Algorithm 2: Construction of High Order Elements using Recursive Towers

Result: Output: A, B (List of orders of Elements).
initialization: $m := 2; p := 11; v := 1;$
$F_{m_0} < z >:= FiniteField(p, m^{(v)});$
$S := [z^4, z^7, z^9, z^{28}, z^{45}, z^{68}, z^{74}, z^{77}, z^{94}, z^{100}, z^{116}]$; (List of Generators of F_{m_0}).
for $y_0 \in S$ **do**
  $F_{m_1} < z >:= FiniteField(p, m^{v+1});$
  $y_1 := elt < F_{m_1} | y_0 >;$
  $P_1 < x >:= PolynomialRing(F_{m_1});$
  $g_1 := x^2 + x - {y_1}^3 + {y_1}^2;$
  $h_1 := Roots(g_1);$
  if $\#h_1 \neq 0$ **then**
    $p_1 := h1[1][1];$
    $d_1 := {p_1}^{m-1};$
    if $p_1 * d_1 = 0$ **then**
      $c := 0;$
      else
        $c := Order(p_1);$
        $a_{01} := Log(2, c);$
        $a_1 := ChangePrecision(a_{01}, 3);$
        $b_{01} := Log(2, Order(d_1));$
        $b_1 := ChangePrecision(b_{01}, 3);$
        $F_{m_2} < z >:= FiniteField(p, m^{v+2});$
        $y_2 := elt < F_{m_2} | p_1 >;$
        $P_2 < x >:= PolynomialRing(F_{m_2});$
        $g_2 := x^2 + x - {y_2}^3 + {y_2}^2;$
        $h_2 := Roots(g_2);$
        if $\#h_2 \neq 0$ **then**
          $p_2 := h_2[1][1];$
          $a_{02} := Log(2, Order(p_2));$
          $a_2 := ChangePrecision(a_{02}, 3);$
          $d_2 := {p_2}^{m-1};$
          $b_{02} := Log(2, Order(d_2));$
          $b_2 := ChangePrecision(b_{02}, 3);$
          $F_{m_3} < z >:= FiniteField(p, m^{v+3});$
          $y_3 := elt < F_{m_3} | p_2 >;$
          $P_3 < x >:= PolynomialRing(F_{m_3});$
          $g_3 := x^2 + x - {y_3}^3 + {y_3}^2;$
          $h_3 := Roots(g_3);$
          if $\#h_3 \neq 0$ **then**
            $p_3 := h_3[1][1];$
            $a_{03} := Log(2, Order(p_3));$
            $a_3 := ChangePrecision(a_{03}, 3);$
            $d_3 := {p_3}^{m-1};$
            $b_{03} := Log(2, Order(d_3));$
            $b_3 := ChangePrecision(b_{03}, 3);$
            $A := [a_1, a_2, a_3];$
            $B := [b_1, b_2, b_3];$
      end
end

Note: This *'sample'* pseudocode is only upto $n = 3$ in the tower of fields $\{GF(p, 2^n)\}_{n\geq 1}$ (compact notation) of odd characteristic p. In the implementation phase, we were able to construct upto $n = 9$ in the tower of fields $\{GF(p, 2^n)\}_{n\geq 1}$ of odd characteristic $p \leq 11$, for which we have provided the numerical result in Appendix C.

Appendix C. Numerical Results for Odd Recursive Towers

In this Appendix, we have collated the multiplicative orders of the element $o(x_n)$, and orders of the discriminant $o(\delta_n)$, for odd p for small n, in the towers defined by $f_i(x_{n-1}, x_n)$, for $i = 1, 2, \ldots, 5$. In most of the cases we obtained generators of the multiplicative groups $\mathrm{GF}(p, 2^n)^*$. We tabulated base two logarithm of the orders as they grow (almost) exponentially. The interested reader can also find the lower and upper bounds for $o(x_n)$ and $o(\delta_n)$ listed in Table 1 for odd characteristic. MAGMA [BoCa93] computational algebra system was used for the experiments. A sample MAGMA code for $p = 11$ can be found here.

Table 1: Lower bound and upper bounds for odd $p \leq 11$.

p	Lower bound	3	5	7	11
n	$\log_2(2^{(n^2+3n)/2})$	$\log_2(p^{2^n}-1)$	$\log_2(p^{2^n}-1)$	$\log_2(p^{2^n}-1)$	$\log_2(p^{2^n}-1)$
1	2.0	3.0	4.6	5.6	6.9
2	5.0	6.3	9.3	11.2	13.8
3	9.0	12.7	18.6	22.5	27.7
4	14.0	25.4	37.2	44.9	55.4
5	20.0	50.7	74.3	89.8	110.7
6	27.0	101.4	148.6	179.7	221.4
7	35.0	202.9	297.2	359.3	442.8
8	44.0	405.8	594.4	718.7	885.6
9	54.0	811.5	1188.8	1437.4	1771.2

Table 2: Results for $f_1(x_{n-1}, x_n)$ for odd $p \leq 11$.

p	3	3	5	5	7	7	11	11
$x_1^2 =$	$2x_1+1$	$2x_1+1$	$3x_1+2$	$3x_1+2$	x_1+4	x_1+4	$4x_1+9$	$4x_1+9$
	LB	UB	LB	UB	LB	UB	LB	UB
n	$\log_2(o(x_n))$	$\log_2(o(\delta_n))$	$\log_2(o(x_n))$	$\log_2(o(\delta_n))$	$\log_2(o(x_n))$	$\log_2(o(\delta_n))$	$\log_2(o(x_n))$	$\log_2(o(\delta_n))$
1	3.0	3.0	4.6	3.0	5.6	5.6	6.9	5.3
2	6.3	6.3	9.3	9.3	11.2	11.2	13.8	13.8
3	12.7	12.7	18.6	18.6	22.5	22.5	27.7	27.7
4	25.4	25.4	37.2	37.2	44.9	44.9	55.4	55.4
5	50.7	50.7	74.3	74.3	89.8	89.8	110.7	110.7
6	101.4	101.4	148.6	148.6	179.7	179.7	221.4	221.4
7	202.9	202.9	297.2	297.2	359.3	359.3	442.8	442.8
8	405.8	405.8	594.4	594.4	718.7	718.7	883.3	885.6
9	811.5	811.5	1188.8	1188.8	1437.4	1437.4	1771.2	1771.2

Table 3: Results for $f_2(x_{n-1}, x_n)$ for odd $p \leq 11$.

p	3	3	5	5	7	7	11	11
$x_1^2 =$	$2x_1+1$	$2x_1+1$	$3x_1+2$	$3x_1+2$	x_1+4	x_1+4	$4x_1+9$	$4x_1+9$
	LB	UB	LB	UB	LB	UB	LB	UB
n	$\log_2(o(x_n))$	$\log_2(o(\delta_n))$	$\log_2(o(x_n))$	$\log_2(o(\delta_n))$	$\log_2(o(x_n))$	$\log_2(o(\delta_n))$	$\log_2(o(x_n))$	$\log_2(o(\delta_n))$
1	3.0	3.0	4.6	4.6	5.6	5.6	6.9	4.6
2	6.3	6.3	9.3	9.3	11.2	11.2	13.8	12.3
3	12.7	12.7	18.6	18.6	20.9	22.5	26.1	27.7
4	25.4	25.4	37.2	37.2	44.9	44.9	55.4	48.9
5	50.7	50.7	74.3	74.3	88.3	89.8	106.6	110.7
6	101.4	101.4	148.6	148.6	179.7	179.7	221.4	219.8
7	202.9	202.9	297.2	297.2	357.8	359.3	441.2	442.8
8	405.8	405.8	594.4	594.4	718.7	718.7	885.6	879.2
9	811.5	811.5	1188.8	1188.8	1435.8	1437.4	1767.1	1771.2

Table 4: Results for $f_3(x_{n-1}, x_n)$ for odd $p \leq 11$.

p	3	3	5	5	7	7	11	11
$x_1^2 =$	$x_1 + 1$	$x_1 + 1$	$2x_1 + 2$	$2x_1 + 2$	$3x_1 + 2$	$3x_1 + 2$	$4x_1 + 9$	$4x_1 + 9$
	LB	UB	LB	UB	LB	UB	LB	UB
n	$\log_2(\mathrm{o}(x_n))$	$\log_2(\mathrm{o}(\delta_n))$	$\log_2(\mathrm{o}(x_n))$	$\log_2(\mathrm{o}(\delta_n))$	$\log_2(\mathrm{o}(x_n))$	$\log_2(\mathrm{o}(\delta_n))$	$\log_2(\mathrm{o}(x_n))$	$\log_2(\mathrm{o}(\delta_n))$
1	3.0	3.0	4.6	4.6	5.6	4.0	6.9	5.3
2	6.3	4.0	9.3	5.6	11.2	5.0	13.8	6.3
3	12.7	5.0	18.6	6.6	22.5	6.0	25.4	7.3
4	25.4	6.0	37.2	7.6	44.9	7.0	51.3	8.3
5	50.7	7.0	74.3	8.6	89.8	8.0	106.6	9.3
6	101.4	8.0	148.6	9.6	179.7	9.0	217.3	10.3
7	202.9	9.0	297.2	10.6	359.3	10.0	436.4	11.3
8	405.8	10.0	594.4	11.6	718.7	11.0	881.5	12.3
9	811.5	11.0	1188.8	12.6	1437.4	12.0	1767.1	13.3

Table 5: Results for $f_4(x_{n-1}, x_n)$ for odd $p \leq 11$.

p	3	3	5	5	7	7	11	11
$x_1^2 =$	$x_1 + 1$	$x_1 + 1$	$4x_1 + 3$	$4x_1 + 3$	$2x_1 + 4$	$2x_1 + 4$	$7x_1 + 4$	$7x_1 + 4$
	LB	UB	LB	UB	LB	UB	LB	UB
n	$\log_2(\mathrm{o}(x_n))$	$\log_2(\mathrm{o}(\delta_n))$	$\log_2(\mathrm{o}(x_n))$	$\log_2(\mathrm{o}(\delta_n))$	$\log_2(\mathrm{o}(x_n))$	$\log_2(\mathrm{o}(\delta_n))$	$\log_2(\mathrm{o}(x_n))$	$\log_2(\mathrm{o}(\delta_n))$
1	3.0	3.0	4.6	4.6	5.6	5.6	6.9	4.6
2	6.3	4.0	9.3	7.7	11.2	11.2	13.8	13.8
3	12.7	5.0	17.0	17.0	22.5	20.9	27.7	27.7
4	25.4	6.0	35.6	37.2	41.0	43.3	55.4	55.4
5	50.7	7.0	72.7	72.7	89.8	89.8	110.7	109.1
6	101.4	8.0	147.0	148.6	177.3	179.7	221.4	219.8
7	202.9	9.0	295.6	295.6	359.3	357.8	442.8	441.2
8	405.8	10.0	592.8	594.4	717.1	717.1	885.6	884.0
9	811.5	11.0	1187.2	1188.8	1435.8	1435.8	1769.6	1771.2

Table 6: Results for $f_5(x_{n-1}, x_n)$ for odd $p \leq 11$.

p	3	3	5	5	7	7	11	11
$x_1^2 =$	$x_1 + 1$	$x_1 + 1$	$x_1 + 3$	$x_1 + 3$	$2x_1 + 2$	$2x_1 + 2$	$4x_1 + 4$	$4x_1 + 4$
	LB	UB	LB	UB	LB	UB	LB	UB
n	$\log_2(\mathrm{o}(x_n))$	$\log_2(\mathrm{o}(\delta_n))$	$\log_2(\mathrm{o}(x_n))$	$\log_2(\mathrm{o}(\delta_n))$	$\log_2(\mathrm{o}(x_n))$	$\log_2(\mathrm{o}(\delta_n))$	$\log_2(\mathrm{o}(x_n))$	$\log_2(\mathrm{o}(\delta_n))$
1	3.0	3.0	4.6	4.6	5.6	5.6	6.9	3.0
2	6.3	4.0	9.3	5.6	8.9	5.0	13.8	5.6
3	12.7	5.0	18.6	8.7	22.5	12.2	27.7	14.8
4	25.4	6.0	35.6	18.0	42.6	23.5	55.4	28.7
5	50.7	7.0	72.7	38.2	89.8	45.9	110.7	56.4
6	101.4	8.0	147.0	73.7	179.7	89.3	221.4	110.1
7	202.9	9.0	295.6	149.6	359.3	179.1	442.8	220.8
8	405.8	10.0	592.8	296.6	718.7	358.8	883.3	442.8
9	811.5	11.0	1187.2	595.4	1437.4	718.1	1771.2	885.0

Table 7: Comparative Analysis

n	$\log_2(\lvert\mathbb{F}^*_{3^{2^n}}\rvert)$	Our Model	Burkhart's Model [*BCGH*+09]	Cohen's Model [Cohen92, Th. 6]
1	3.0	3.0	3.0	3.0
2	6.3	6.3	5.3	4.0
3	12.7	12.7	10.7	5.0
4	25.4	25.4	22.4	6.0
5	50.7	50.7	46.8	7.0
6	101.4	101.4	96.5	8.0
7	202.9	202.9	197.0	9.0
8	405.8	405.8	399.0	10.0
9	811.5	811.5	804.0	11.0

Appendix D. Computational Results for Class Number Estimation

Table 8: Class Number Table.

Class No.	Primes	Sum (S)
1	7, 11, 19, 43, 67, 163	14, 44, 152, 860, 2144, 13040
3	23, 31, 59, 83, 107, 139, 211, 283, 307, 331, 379, 499, 547, 643, 883, 907	184, 372, 1534, 3154, 5350, 9174, 21522, 39054, 46050, 53622, 70494, 122754, 147690, 204474, 386754, 408150
5	47, 79, 103, 127, 131, 179, 227, 347, 443, 523, 571, 619, 683, 691, 739, 787, 947	846, 2686, 4738, 7366, 7860, 15036, 24516, 58296, 95688, 133888, 159880, 188176, 229488, 234940, 268996, 305356, 443196
7	71, 151, 223, 251, 463, 467, 487, 587, 811, 827, 859	1988, 10268, 23192, 29618, 103712, 105542, 114932, 167882, 322778, 335762, 362498
9	199, 367, 419, 491, 563, 823	17910, 63858, 83800, 115876, 153136, 330846
11	167, 271, 659, 967	12024, 33604, 209562, 456424
13	191, 263, 607, 631, 727	15662, 31034, 176030, 190562, 254450
15	239, 439, 751, 971	24856, 89556, 270360, 456370
17	383, 991	66642, 473698
19	311, 359, 919	42296, 57440, 404360
21	431, 503, 743, 863	83614, 115690, 260050, 353830
23	647	194100
25	479, 599	102506, 164126
27	983	456112
29	887	367218
31	719, 911	235832, 386264
33	839	323854

Some Related Academic Works

1. *High Order Elements in Finite Fields and Modular Curve Towers*

This is a joint work of the PhD candidate Ankan Pal, with Kalyan Banerjee, Pietro Mercuri, Valerio Dose, and Claudio Stirpe.

A peculiar relationship between recursive equations derived by Elkies in [Elki01] of modular curve towers to construct/find elements of high order in a finite field was found by Burkhart et. al. in [$BCGH^{+}09$]. But, they did not entail the reason for such a behavior. In this research work, we delve deeper into understanding the reason behind this peculiar phenomena. The recursive relationships derived by Elkies were for towers of modular curves of level 0 ($\{X_0(2^n)_{n\geq 1}\}$). A natural question arises that, can we find similar parametrization for the towers of modular curves of level 1. We modify the method of isogenies from [Elki01], and derive a lemma for the product of maps. Using that, we show the equivalence of $\{X_1(2^n)_{n\geq 1}\}$ and $\{X_0(2^n)_{n\geq 1}\}$ Modular Curve Tower(s). We state the main result of this research work here.

Theorem (Equivalence of Modular Towers). The recursive equations of the modular curve tower $\{X_1(2^n)\}_{n\geq 1}$ and $\{X_0(2^n)\}_{n\geq 1}$ are identical, if the method of isogenies (proposed by Elkies in [Elki01]) is used.

2. *Evaluation of Hasse-Weil L-function for Certain Families of Elliptic Curves at $s = 1$*

This is a joint work of the PhD candidate Ankan Pal, with Bidisha Roy, and Abhishek Juyal.

In this research work, we elucidated that how the Edwards Curves and their twists can be useful in evaluating special values of L-function. The result is about evaluating Hasse-Weil L-function $L(E, s)$ at $s = 1$, of an elliptic curve E over $\mathbb{Q}$.

In 1979, Williams [Will79] also considers applying his transformation formulas (3.3.1) to elliptic curves defined over the rationals and having complex multiplication. Coincidentally, the quadratic forms that are used in his transformation formula can be modified in such a way that we get the Edwards Curve, which first appeared in the literature in 2007 [Edwa07]. Motivated by this, we derive some trace formulas. We also explore the possibility of leveraging these ideas to calculate some special values of Hasse-Weil L-functions of an elliptic curve over $\mathbb{Q}$. We state the main result of this research work here.

Theorem (Evaluation of L-function at $s = 1$). Let, $E_{Ed} : y^2 = \frac{ax^2-1}{dx^2-1}$ be a twisted Edwards curve and $E'_{Ed} : y^2 = \frac{x^2-a^2}{a^2dx^2-1}$ be an Edwards curve over $\mathbb{Q}$. Also, let, $E : y^2 = x(x-1)\left(x - \frac{a}{d}\right)$ and $E' : y^2 = x^3 - \frac{1+a^4d}{a^2}x^2 + \frac{1}{d}x$ be elliptic curves over $\mathbb{Q}$. Lets choose odd primes p for which E and E' have good reduction, such that for all the curves $a \not\equiv d \not\equiv 0 \ (mod\ p)$. Additionally, if, for E and E_{Ed} we consider the odd primes p for which $dx^2 - 1 \not\equiv 0 \ (mod\ p)$; and for E' and E'_{Ed}, $a^2dx^2 - 1 \not\equiv 0 \ (mod\ p)$. Then,

$$L(E, 1) = \prod_{good\ p} \frac{p}{p - \left(\frac{d}{p}\right) tr(E_{Ed}) + \left(\frac{a}{p}\right) + 1}$$

and

$$L(E', 1) = \prod_{good\ p} \frac{p}{p - \left(\frac{d}{p}\right) tr(E'_{Ed}) + 2}.$$

Where, $tr(.)$ is the trace of the respective Edwards curves and $\left(\frac{\cdot}{p}\right)$ is the usual Legendre Symbol.

3. *Generalization of Lattice based Cryptography on Hypercomplex Algebras*

This is a joint work of the PhD candidate Ankan Pal with Sonika Singh, and Sahadeo Padhye, which is completed and accepted in International Conference on Security and Privacy, 2020.

Abstract. In this research work, we illustrate on the possibility of providing a generalized framework for the implementation of lattice-based cryptosystems using higher dimensional Hypercomplex Numbers, obtained through the Cayley-Dickson method. A framework consisting of the necessary assumptions on invertibility, modularity, norms and zero-divisors were elucidated. A random allocation of the resulting hierarchy was proposed for various application scenarios. The hierarchies which were presented, tend to be secure to the attacks by a quantum adversary. An instantiation named as **STRU**, which is an analogue of the **NTRU** cryptosystem, over a 16-dimensional Sedenion algebra, was provided. We anticipate that it might find an application in the advent of Post-Quantum era. An interesting property which is coined as Inverse Associative Property for the basis elements of the Sedenion Algebra was verified through computational methods, which is needed for the implementation of STRU.

List of Preprints

(1) A New Method for Geometric Interpretation of Elliptic Curve Discrete Logarithm Problem.

Authors: *Daniele Di Tullio, Ankan Pal*.

Status: Completed. Available on arXiV.

(2) High Order Elements in Finite Fields Arising from Recursive Towers.

Authors: *Valerio Dose, Pietro Mercuri, Ankan Pal, Claudio Stirpe*.

Status: Completed. Available on arXiV.

(3) Supersingular Isogeny-based Designated Verifier Blind Signature.

Authors: *Rajeev Anand Sahu, Agnese Gini, Ankan Pal*.

Status: Completed. Available on IACR.

Citations: 5.

(4) Evaluation of Hasse-Weil L-function for Certain Families of Elliptic Curves at $s = 1$.

Authors: *Ankan Pal, Bidisha Roy, Abhishek Juyal*.

Status: Submitted.

(5) High Order Elements in Finite Fields and Modular Curve Towers.

Collaborators: *Kalyan Banerjee, Valerio Dose, Pietro Mercuri, Ankan Pal, Claudio Stirpe*.

Status: Completed. Not submitted.

(6) Generalization of Lattice based Cryptography on Hypercomplex Algebras.

Authors: *Sonika Singh, Sahadeo Padhye, Ankan Pal*.

Status: Completed. Accepted in International Conference on Security and Privacy, 2020.

Bibliography

[AAB919] Arute, F., Arya, K., Babbush, R., Bacon, D., Bardin, J.C., Barends, R., Biswas, R., Boixo, S., Brandao, F.G., Buell, D.A. and Burkett, B., 2019. Quantum supremacy using a programmable superconducting processor. Nature, 574(7779), pp.505-510.

[AeCa17] Aebi, C. and Cairns, G., 2017. Sums of quadratic residues and nonresidues. The American Mathematical Monthly, 124(2), pp.166-169.

[AhSh10] O. Ahmadi and I. E. Shparlinski, Bilinear character sums and the sum-product problem on elliptic curves, Proc. Edinburgh Math. Soc., 53 (2010), 1–12.

[$BCGH^{+}09$] Burkhart, J.F., Calkin, N.J., Gao, S., Hyde-Volpe, J.C., James, K., Maharaj, H., Manber, S., Ruiz, J. and Smith, E., 2009. Finite field elements of high order arising from modular curves. Designs, Codes and Cryptography, 51(3), pp.301-314.

[BeKV19] Beullens, W., Kleinjung, T. and Vercauteren, F., 2019, December. CSI-FiSh: Efficient isogeny based signatures through class group computations. In International Conference on the Theory and Application of Cryptology and Information Security (pp. 227-247). Springer, Cham.

[BeTa17] Bernstein Daniel, J. and Tanja, L., 2017. Post-quantum cryptography. Nature, 549(7671), pp.188-194.

[BLMS00] Brassard, G., Lütkenhaus, N., Mor, T. and Sanders, B.C., 2000. Limitations on practical quantum cryptography. Physical Review Letters, 85(6), p.1330.

[BoCa93] Bosma, W. and Cannon, J., 1993. MAGMA handbook. University of Sydney.

[BuTV04] Buchmann, J., Takagi, T. and Vollmer, U., 2004. Number field cryptography. High Primes and Misdemeanours: Lectures in Honour of the 60th Birthday of Hugh Cowie Williams, van der Poorten and Stein, eds, 41, pp.111-125.

[BuWi88] Buchmann, J. and Williams, H.C., 1988. A key-exchange system based on imaginary quadratic fields. Journal of Cryptology, 1(2), pp.107-118.

[CaLa09] Castagnos, G. and Laguillaumie, F., 2009, April. On the security of cryptosystems with quadratic decryption: the nicest cryptanalysis. In Annual International Conference on the Theory and Applications of Cryptographic Techniques (pp. 260-277). Springer, Berlin, Heidelberg.

[CaLa15] Castagnos, G. and Laguillaumie, F., 2015, April. Linearly homomorphic encryption from DDH. In Cryptographers' Track at the RSA Conference (pp. 487-505). Springer, Cham.

[Cast08] Castagnos, G., 2008, September. Two Generic Constructions of Probabilistic Cryptosystems and Their Applications. In International Conference on Security and Cryptography for Networks (pp. 92-108). Springer, Berlin, Heidelberg.

[Cast19] Castagnos, G., 2019. Cryptography based on quadratic fields: cryptanalyses, primitives and protocols (Doctoral dissertation, Université de Bordeaux).

[Chang13] Mei-Chu Chang, Elements of large order in prime finite fields, Bull. Aust. Math. Soc. 88 (2013), no. 1, 169–176. MR 3096879.

[Chap97] Chapman, R., 1997. Completely normal elements in iterated quadratic extensions of finite fields. Finite Fields and Their Applications, 3(1), pp.1-10.

[Chaum83] Chaum, D., 1983. Blind signatures for untraceable payments. In Advances in cryptology (pp. 199-203). Springer, Boston, MA.

[ChLG09] Charles, D.X., Lauter, K.E. and Goren, E.Z., 2009. Cryptographic hash functions from expander graphs. Journal of Cryptology, 22(1), pp.93-113.

[ChVa89] Chaum, D. and Van Antwerpen, H., 1989, August. Undeniable signatures. In Conference on the Theory and Application of Cryptology (pp. 212-216). Springer, New York, NY.

[Cohen92] Cohen, S.D., 1992. The explicit construction of irreducible polynomials over finite fields. Designs, Codes and Cryptography, 2(2), pp.169-174.

[Cohn12] Cohn, H., 2012. Advanced Number Theory. Courier Corporation.

[Con01] Alessandro Conflitti, On elements of high order in finite fields, Cryptography and computational number theory (Singapore, 1999), Progr. Comput. Sci. Appl. Logic, vol. 20, Birkhäuser, Basel, 2001, pp. 11–14. MR 1944714.

[Cox11] Cox, D.A., 2011. Primes of the form $x^2 + ny^2$: Fermat, class field theory, and complex multiplication (Vol. 34). John Wiley and Sons.

[Dave00] Harold Davenport, Multiplicative number theory, volume 74 of Graduate Texts in Mathematics. Springer-Verlag, New York, third edition, 2000. Revised and with a preface by Hugh L. Montgomery.

[DeGB87] Desmedt, Y., Goutier, C. and Bengio, S., 1987, August. Special uses and abuses of the Fiat-Shamir passport protocol. In Conference on the Theory and Application of Cryptographic Techniques (pp. 21-39). Springer, Berlin, Heidelberg.

[DeYu91] Desmedt, Y. and Yung, M., 1991, April. Weaknesses of undeniable signature schemes. In Workshop on the Theory and Application of of Cryptographic Techniques (pp. 205-220). Springer, Berlin, Heidelberg.

[Diem13] Diem, C., 2013. On the discrete logarithm problem in elliptic curves II. Algebra and Number Theory, 7(6).

[DiGS06] Ding, J., Gower, J.E. and Schmidt, D., 2006. Zhuang-Zi: A New Algorithm for Solving Multivariate Polynomial Equations over a Finite Field. IACR Cryptology ePrint Archive, 2006, p.38.

[Edwa07] Harold Edwards. A normal form for elliptic curves. Bulletin of the American mathematical society, 44(3):393–422, 2007.

[El18] El Housni, Y., 2018. Introduction to the Mathematical Foundations of Elliptic Curve Cryptography.

[Elki01] Elkies, N.D., 2001. Explicit modular towers. arXiv preprint math/0103107.

[Faug99] Faugere, J.C., 1999. A new efficient algorithm for computing Gröbner bases (F4). Journal of pure and applied algebra, 139(1-3), pp.61-88.

[FeJP14] De Feo, L., Jao, D. and Plut, J., 2014. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. Journal of Mathematical Cryptology, 8(3), pp.209-247.

[Feyn86] Feynman, R.P., 1986. Quantum mechanical computers. Foundations of physics, 16(6), pp.507-531.

[FiSh86] Fiat, A. and Shamir, A., 1986, August. How to prove yourself: Practical solutions to identification and signature problems. In Conference on the Theory and Application of Cryptographic Techniques (pp. 186-194). Springer, Berlin, Heidelberg.

[Flynn90] Flynn, E.V., 1990, May. The Jacobian and formal group of a curve of genus 2 over an arbitrary ground field. In Mathematical Proceedings of the Cambridge Philosophical Society (Vol. 107, No. 3, pp. 425-441). Cambridge University Press.

[Ful08] Fulton, W., 2008. Algebraic curves. An Introduction to Algebraic Geom, p.54.

[Gao99] S. Gao, Elements of provable high orders in finite fields, Proceedings of the American Mathematical Society 127 (1999), no. 6, 1615–1623.

[GaPS17] Galbraith, S.D., Petit, C. and Silva, J., 2017, December. Identification protocols and signature schemes based on supersingular isogeny problems. In International Conference on the Theory and Application of Cryptology and Information Security (pp. 3-33). Springer, Cham.

[GaSh95] J. Gathen and I. Shparlinski, Orders of gauss periods in finite fields, Algorithms and Computations, 1995.

[GaSh01] Joachim von zur Gathen and Igor Shparlinski, Gauss periods in finite fields, Finite fields and applications (Augsburg, 1999), Springer, Berlin, 2001, pp. 162–177. MR 1849087.

[GaSm99] Galbraith, S.D. and Smart, N.P., 1999, December. A cryptographic application of Weil descent. In IMA International Conference on Cryptography and Coding (pp. 191-200). Springer, Berlin, Heidelberg.

[Gaud09] Gaudry, P., 2009. Index calculus for abelian varieties of small dimension and the elliptic curve discrete logarithm problem. Journal of Symbolic Computation, 44(12), pp.1690-1702.

[GGP98] Gao, S., Von Zur Gathen, J. and Panario, D., 1998. Gauss periods: orders and cryptographical applications. Mathematics of Computation, 67(221), pp.343-352.

[Hart13] Hartshorne, R., 2013. Algebraic geometry (Vol. 52). Springer Science and Business Media.

[HoLW06] Hoory, S., Linial, N. and Wigderson, A., 2006. Expander graphs and their applications. Bulletin of the American Mathematical Society, 43(4), pp.439-561.

[HJPT98] Huhnlein, D., Jacobson, M.J., Paulus, S. and Takagi, T., 1998, May. A cryptosystem based on non-maximal imaginary quadratic orders with fast decryption. In International Conference on the Theory and Applications of Cryptographic Techniques (pp. 294-307). Springer, Berlin, Heidelberg.

[HoPS98] J. Hoffstein, J. Pipher and J. H. Silverman, NTRU: a ring based public key cryptosystem, in: Proc. of ANTS, LNCS, vol-1423, pp. 267-288, Springer, 1998.

[Huse87] Husemoller, D., 1987. Elliptic curves, volume 111 of. Graduate Texts in Mathematics, p.99.

[IrRo67] K. Ireland and M. Rosen, A Classical Introduction to Modern Number Theory. Graduate Texts in Mathematics, 87; Van der Waerden, B.L. and Algebra, I., Springer-Verlag, Berlin-Heidelberg-New York, 1967.

[Jakob94] Jakobsson, M., 1994, May. Blackmailing using undeniable signatures. In Workshop on the Theory and Application of of Cryptographic Techniques (pp. 425-427). Springer, Berlin, Heidelberg.

[JaSI96] Jakobsson, M., Sako, K. and Impagliazzo, R., 1996, May. Designated verifier proofs and their applications. In International Conference on the Theory and Applications of Cryptographic Techniques (pp. 143-154). Springer, Berlin, Heidelberg.

[JaSo14] Jao, D. and Soukharev, V., 2014, October. Isogeny-based quantum-resistant undeniable signatures. In International Workshop on Post-Quantum Cryptography (pp. 160-179). Springer, Cham.

[JaSW08] Jacobson, M.J., Scheidler, R. and Weimer, D., 2008, June. An adaptation of the NICE cryptosystem to real quadratic orders. In International Conference on Cryptology in Africa (pp. 191-208). Springer, Berlin, Heidelberg.

[Klai12] Klaise, Janis, 2012. Orders in quadratic imaginary fields of small class number. Notes (Preprint). Retrieved from https://warwick.ac.uk on February 18, 2021.

[KMPPS20] Kutas, P., Martindale, C., Panny, L., Petit, C. and Stange, K.E., 2020. Weak instances of SIDH variants under improved torsion-point attacks. arXiv preprint arXiv:2005.14681.

[Kobl12] Koblitz, N., 2012. Algebraic aspects of cryptography (Vol. 3). Springer Science and Business Media.

[Mcel78] McEliece, R.J., 1978. A public-key cryptosystem based on algebraic. Coding Thv, 4244, pp.114-116.

[McRa12] McLeman, C. and Rasmussen, C., 2012. Class number formulas via 2-isogenies of elliptic curves. Bulletin of the London Mathematical Society, 44(6), pp.1221-1236.

[Merk79] Merkle, R., 1979. Secrecy, authentication, and public key systems. Ph. D. Thesis, Stanford University.

[Meyn95] Meyn, H., 1995. Explicit N-polynomials of 2-power degree over finite fields, I. Designs, Codes and Cryptography, 6(2), pp.107-116.

[MOV93] Menezes, A.J., Okamoto, T. and Vanstone, S.A., 1993. Reducing elliptic curve logarithms to logarithms in a finite field. IEEE Transactions on information Theory, 39(5), pp.1639-1646.

[MuPa13] Mullen, G.L. and Panario, D., 2013. Handbook of finite fields. CRC Press.

[Onl1] Retrieved from https://quantumexperience.ng.bluemix.net on June 03, 2019.

[Onl2] Retrieved from https://csrc.nist.gov (Round 1 Submissions) on June 03, 2019.

[Onl3] Retrieved from https://csrc.nist.gov (Round 2 Submissions) on June 03, 2019.

[Onl4] Retrieved from https://csrc.nist.gov (Round 3 Submissions) on September 03, 2020.

[Pail99] Paillier, P., 1999, May. Public-key cryptosystems based on composite degree residuosity classes. In International conference on the theory and applications of cryptographic techniques (pp. 223-238). Springer, Berlin, Heidelberg.

[PaPe09] Paar, C. and Pelzl, J., 2009. Understanding cryptography: a textbook for students and practitioners. Springer Science and Business Media.

[Pata96] Patarin, J., 1996, May. Hidden fields equations (HFE) and isomorphisms of polynomials (IP): Two new families of asymmetric algorithms. In International Conference on the Theory and Applications of Cryptographic Techniques (pp. 33-48). Springer, Berlin, Heidelberg.

[PeLa17] Petit, C. and Lauter, K.E., 2017. Hard and Easy Problems for Supersingular Isogeny Graphs. IACR Cryptology ePrint Archive, 2017, p.962.

[Petit17] Petit, C., 2017, December. Faster algorithms for isogeny problems using torsion point images. In International Conference on the Theory and Application of Cryptology and Information Security (pp. 330-353). Springer, Cham.

[Poll78] Pollard, J.M., 1978. Monte Carlo methods for index computation (mod p) Mathematics of computation, 32(143), pp.918-924.

[Popov12] R. Popovych, Elements of high order in finite fields of the form $\mathbb{F}_q[\chi]/\phi_r(\chi)$, Finite Fields Appl. 18 (2012), no. 4, 700–710. MR 2928465.

[Popov13] R. Popovych, Elements of high order in finite fields of the form $\frac{\mathbb{F}_q[\chi]}{\chi^m-a}$, Finite Fields Appl. 19 (2013), 86–92. MR 2996762.

[Popov14A] R. Popovych On elements of high order in general finite fields, Algebra Discrete Math. 18 (2014), no. 2, 295–300. MR 3352714.

[Popov14B] R. Popovych Sharpening of the explicit lower bounds for the order of elements in finite field extensions based on cyclotomic polynomials, Ukrainian Math. J. 66 (2014), no. 6, 916–927, Reprint of Ukraïn. Mat. Zh. 66 (2014), no. 6, 815–825. MR 3284597.

[Popov15A] R. Popovych, On the multiplicative order of elements in Wiedemann's towers of finite fields, Carpathian Math. Publ. 7 (2015), no. 2, 220–225. MR 3457907.

[Popov18] R. Popovych, Multiplicative orders of elements in Conway's towers of finite fields, Algebra Discrete Math. 25 (2018), no. 1, 137–146. MR 3798300.

[PopSku20] Popovych, R. and Skuratovskii, R., 2020. Normal high order elements in finite field extensions based on the cyclotomic polynomials. Algebra and Discrete Mathematics, 29(2).

[PoSt00] Pointcheval, D. and Stern, J., 2000. Security arguments for digital signatures and blind signatures. Journal of cryptology, 13(3), pp.361-396.

[Reg09] Regev, O., 2009. On lattices, learning with errors, random linear codes, and cryptography. Journal of the ACM (JACM), 56(6), p.34.

[Scho95] René Schoof. Counting points on elliptic curves over finite fields. Journal de théorie des nombres de Bordeaux, 7(1):219–254, 1995.

[ScUn17] Schröder, D. and Unruh, D., 2017. Security of blind signatures revisited. Journal of Cryptology, 30(2), pp.470-494.

[Sema04] Semaev, I.A., 2004. Summation polynomials and the discrete logarithm problem on elliptic curves. IACR Cryptology ePrint Archive, 2004, p.31.

[Shor94] Shor, P.W., 1994, November. Algorithms for quantum computation: Discrete logarithms and factoring. In Proceedings 35th annual symposium on foundations of computer science (pp. 124-134). Ieee.

[Shpar12] I. Shparlinski, Computational and algorithmic problems in finite fields, vol. 88, Springer Science and Business Media, 2012.

[ShRe94] Shafarevich, I.R. and Reid, M., 1994. Basic algebraic geometry (Vol. 2). Berlin: Springer-Verlag.

[Sil09] Silverman, J.H., 2009. The arithmetic of elliptic curves (Vol. 106). Springer Science and Business Media.

[Souk16] Soukharev, V., 2016. Post-quantum elliptic curve cryptography.

[SrCh16] Srinath, M.S. and Chandrasekaran, V., 2016. Isogeny-based Quantum-resistant Undeniable Blind Signature Scheme. IACR Cryptology ePrint Archive, 2016, p.148.

[Sti09] Stichtenoth, H., 2009. Algebraic function fields and codes (Vol. 254). Springer Science and Business Media.

[Stol12] Stolbunov, A., 2012. Cryptographic schemes based on isogenies.

[SuTW12] Sun, X., Tian, H. and Wang, Y., 2012, September. Toward quantum-resistant strong designated verifier signature from isogenies. In 2012 Fourth International Conference on Intelligent Networking and Collaborative Systems (pp. 292-296). IEEE.

[Tate66] Tate, J., 1966. Endomorphisms of abelian varieties over finite fields. Inventiones mathematicae, 2(2), pp.134-144.

[Unruh15] Unruh, D., 2015, April. Non-interactive zero-knowledge proofs in the quantum random oracle model. In Annual International Conference on the Theory and Applications of Cryptographic Techniques (pp. 755-784). Springer, Berlin, Heidelberg.

[Velu71] Velu, J., 1971. Isogenies entre courbes elliptiques. CR Acad. Sci. Paris, Séries A, 273, pp.305-347.

[Vol07] José Felipe Voloch, On the order of points on curves over finite fields, Integers 7 (2007), A49, 4. MR 2373111.

[Vol10] José Felipe Voloch, Elements of high order on finite fields from elliptic curves, Bull. Aust. Math. Soc. 81 (2010), no. 3, 425–429. MR 2639857.

[Wash03] Washington, L.C., 2003. Elliptic curves: number theory and cryptography. Chapman and Hall/CRC.

[Will70] Kenneth S Williams. Finite transformation formulae involving the legendre symbol. Pacific Journal of Mathematics, 34(2):559–568, 1970.

[Will79] Kenneth S Williams. Evaluation of character sums connected with elliptic curves. Proceedings of the American Mathematical Society, 73(3):291–299, 1979.

[YAJJS17] Yoo, Y., Azarderakhsh, R., Jalali, A., Jao, D. and Soukharev, V., 2017, April. A post-quantum digital signature scheme based on supersingular isogenies. In International Conference on Financial Cryptography and Data Security (pp. 163-181). Springer, Cham.

Index

Acknowledgments

I want to acknowledge the love, great efforts, and kind support of my parents, **Mr Amar Kanti Pal and Mrs Ratna Pal**, who were being supportive and patient throughout my academic career.

I want to acknowledge the contribution of **Prof Norberto Gavioli** towards guiding and advising this thesis. I am grateful to the fruitful and illuminating discussions with him. He was the main motivation and a pivotal driving force for the thesis. I want to thank him for his guidance, advice and contribution towards the thesis.

I am grateful to the PhD coordinators at University of L'Aquila, *Professor Davide Gabrielli* and *Professor Anna De Masi*, who helped with the necessary coordination and bureaucratic processes, regarding the PhD.

I would like to thank *Dr Donato Pera* and the High Performance Computing facility of University of L'Aquila, which enabled us to implement many algorithms on MAGMA and run the experiments to validate our results.

I am particularly thankful to *Ms Rossana Rotondi* and the doctoral office of University of L'Aquila, for their help and support during my PhD.

I would like to thank *Professor Kalyan Chakraborty* for arranging my research visit to Harish-Chandra Research Institute (HRI), Prayagraj, India. I would like to thank him for his time and attention during my visit to the institute.

During my stay at HRI, I collaborated with *Dr Abhishek Juyal*, *Dr Bidisha Roy*, and *Mr Krishnarjun*. They all have been good friends and have enlightened me with their knowledge.

A special word of thanks to *Dr Kalyan Banerjee* from HRI, for introducing the concept of Marked Points and his inputs regarding the $\{X_1(2^n)\}_{n\geq 1}$ Modular Curve Tower.

I would like to thank *Dr Pietro Mercuri*, working at University of Rome - La Sapienza, *Dr Claudio Stirpe*, and *Dr Valerio Dose* to collaborate with me on finding connections between recursive towers and high order elements in finite field. This was a mathematically challenging work and it made me question and explore various parts of Mathematics.

Next, I want to thank *Dr Rajeev Anand Sahu* (whom I met at the Elliptic Curve Cryptography Conference - 2017) and *Ms Agnese Gini*, working at University of Luxembourg who gave me the opportunity to collaborate with them on development of the 2-cube method used in the development of the Supersingular Isogeny-Based Designated Verifier Digital Signature.

I would like to thank *Mr Daniele Di Tullio* from Roma Tre University, with whom I worked on a novel geometric interpretation of Elliptic Curve Discrete Logarithm Problem.

I want to thank *Prof Sahadeo Padhye* and his student *Dr Sonika Singh* from Motilal Nehru National Institute of Technology, Prayagraj who showed interest in my work on Lattice-Based Cryptography and entrusted me with the development of a sound mathematical structure using the Sedenion Algebra, so that a NTRU-type cryptographic protocol could be implemented.

I would like to thank *Ms Maria Teresa Grifa*, working at University of L'Aquila, and *Dr Anurag Ranjan* for their collaboration on the quantum attacks on Machine Learning.

During my PhD journey, a pivotal role was played by my collaborators. I want to thank each one of them once again, and convey my gratitude towards them.

I would like to thank my friend **Mr Sudip Sinha** from Louisiana State University, USA with whom I had many illuminating discussions about Mathematics and life, and I am grateful to him for his help and support.

I would like to thank my friend **Mr Anirudh Gupta** who always startles me with his creative energy.

I would like to thank my friend **Mr Ankur Jalan**, who has guided me through thick and thin in my professional and personal life.

I would like to also thank my friend **Mr Prasenjit Paul** and **Mr Badal Yadav**, who always encouraged me during the anxious moments of my life.

I want to thank my three flat-mates during my PhD, *Ms Antonella Lombardi*, *Mr Jorge Oswaldo Regalado Lopez*, and *Mr Manoj Gyawali*, who at times have provided me with the social touch that is indeed needed for sanity.

I would like to thank my friend *Ms Morgana Pintarelli*, who was a great emotional support to me.

I would like to thank my friend and colleague *Dr Monia Capanna*, who helped me during my personal, emotional, and professional dilemmas.

The acknowledgment section would not be complete without the special mention of my dear friend *Ms Vidhi Patel*, who pushed me towards great philosophical dilemmas. Nonetheless, she also illuminated me with the vagaries of life and expedited the process of understanding my priorities.

During my stay in L'Aquila, from November 2016 to April 2018, I had the good fortune of being surrounded by supportive friends and colleagues. I want to acknowledge and thank them for their help and support.

From the bottom of my heart, I want to express my gratitude to all my family, classmates, friends, teachers, doctors, and employers whom I met in Rome, L'Aquila, Ahmedabad, Mumbai, Bangalore, Mangalore, Kolkata, Guwahati, Prayagraj, and Nagpur.

Lastly, I would like to thank my alma-mater University of L'Aquila, Italy and National Institute of Technology Karnataka, Suratkal, India, which provided me with the platform where I could pursue my academic career.

I would to like to thank the researchers in Mathematical community and Cryptographers (whose work I have used (referenced) or otherwise), who have enabled the world to see the elegance of Mathematical structures.

Conclusively, I would like to express my gratitude to all the people, books, research papers, and events in my life which encouraged me to pursue this path.

I would like to thank (in advance) to the reviewers and readers of this thesis who would be taking painstaking effort for reading this thesis.

In 2020, we are experiencing unprecedented times. A pandemic which shook the whole world. Amidst, CoViD-19, the frontline healthcare warriors relentlessly continue working towards saving lives. I want to express my utmost gratitude towards them for their service to mankind.

Quis Custodiet Ipsos Custodes!

"Who will watch the watchmen?"

- Juvenal
circa 128 AD